Le Brexit peut-il avoir un impact sur la cybersécurité, au Royaume-Uni et ailleurs ?

Daniel Ventre, CNRS (CESDIP), Titulaire de la Chaire Cybersécurité & Cyberdéfense

15 Juillet 2016, article III - 25

Le 23 juin 2016 les britanniques étaient appelés à décider du sort de la présence du Royaume-Uni au sein de l'Union Européenne. Les résultats annoncés le 24 juin 2016 ont confirmé le succès des partisans du Brexit (52% contre 48%). Le 13 juillet, la conservatrice Theresa May était nommée premier ministre. Elle aura en charge la gestion de la procédure de retrait du Royaume-Uni de l'Union Européenne.

Bien avant les élections et leurs résultats, les analystes ont tenté de comprendre quels seraient à court, moyen et long terme, les effets de ce retrait tant pour le Royaume-Uni, que pour l'Union Européenne et le reste du monde, sur le plan économique, financier, commercial, ou encore social, migratoire[1].

Anticipant l'annonce des résultats, les chutes des indices boursiers ou de la parité de la Livre Sterling furent parmi les premiers effets. Suivit la baisse de la note accordée par Standard & Poor's au Royaume-Uni. Suivit également une relativement courte période d'incertitude politique, les promoteurs du Brexit refusant de prendre alors le leadership du gouvernement.

Des interrogations doivent désormais être soulevées sur le sujet sécuritaire. L'un des arguments clefs des partisans du Brexit portait précisément sur la sécurité : quitter l'UE devait permettre au Royaume-Uni de retrouver son entière souveraineté et d'être ainsi mieux armé, ayant les mains libres, pour affronter le phénomène migratoire, défendre ses frontières, son espace national. Un peu comme si se retirer de l'UE protégeait des problématiques de la mondialisation, des effets de la globalisation.

Notre article pose la question plus particulière des effets du Brexit sur la cybersécurité, qui appelle des réponses très partagées, positives[2] chez les uns, ou au contraire pessimistes pour d'autres[3]. La cybersécurité est ici observée du point de vue économique (industrie, coût de la lutte contre la

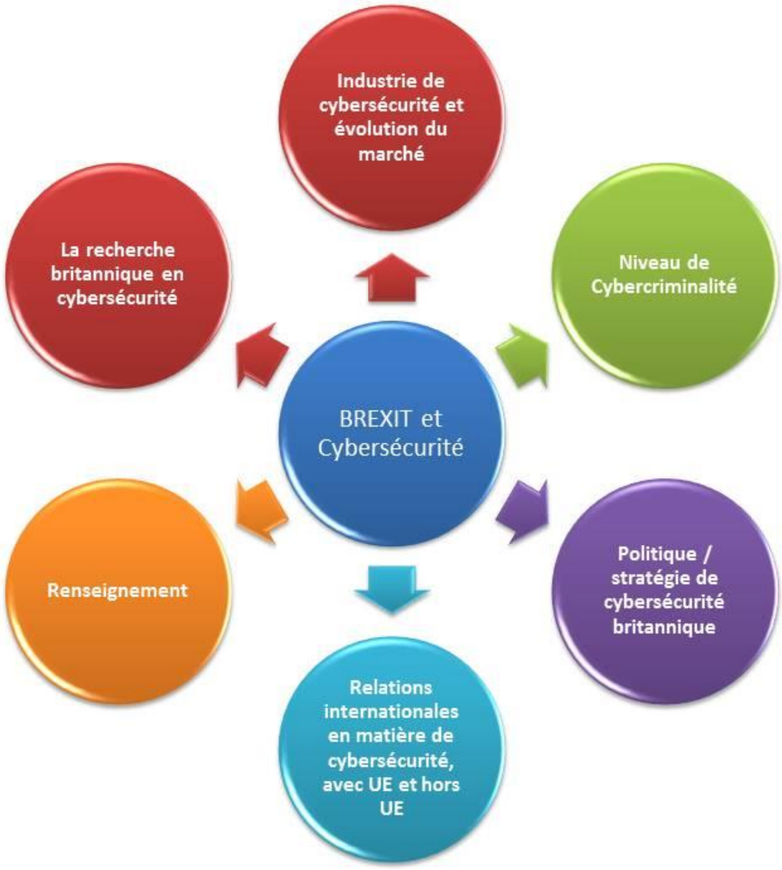
---

[1] Vaughne Miller, « Exiting the EU : impact in key UK policy areas", Briefing Paper, n°07213, 12 février 2016, 161 pages, House of Commons Library, http://researchbriefings.files.parliament.uk/documents/CBP-7213/CBP-7213.pdf

[2] « Cyber Brexit : the chance for a cybersecurity renaissance", 25 juin 2016, site ThreatGeek, http://www.threatgeek.com/2016/06/cyber-brexit-the-chance-for-a-cybersecurity-renaissance.html

[3] http://www.ibtimes.co.uk/how-will-brexit-affect-cybersecurity-uk-what-experts-are-saying-about-leaving-eu-1567008

cybercriminalité), et politique (les perspectives du nouveau gouvernement, et les interactions entre les politiques nationales et le niveau international).



Effets du Brexit sur la cybersécurité : quelques points clefs à observer

1 – L'économie

1.1. L'industrie

Comme toutes les autres activités économiques, l'industrie de la cybersécurité, sera probablement soumise aux effets des transformations induites par le Brexit, que ce soit en raison des évolutions réglementaires au sein même du Royaume-Uni ou des modifications de la relation au marché unique. Quelques variables sont susceptibles de produire des effets :

- l'industrie a pu bénéficier d'aides européennes, qui ne lui seront désormais plus accessibles. Pensons simplement aux subventions accordées par l'UE à la R&D par le biais des programmes cadres. Ces subventions feront autant défaut à l'industrie qu'à la recherche académique, et rien n'assure que le gouvernement britannique sache se substituer à ces sources de revenus conséquents.
- l'industrie a profité des règles du marché unique et de la libre circulation des biens, des capitaux et des individus. Les restrictions qui s'appliqueront désormais constitueront autant de freins à cette liberté d'action, qui contribuait à alimenter l'industrie en ressources humaines (talents) notamment. Les restrictions rendent le Royaume-Uni potentiellement moins attractif.

- L'attractivité du marché et de l'industrie britannique sera pénalisée par l'augmentation des coûts qui va peser sur l'emploi et le commerce (nécessité de visas pour les étrangers, taxes, augmentation du coût des transactions avec les pays européens, etc.) [4]
- Si les entreprises actuellement localisées au Royaume-Uni décidaient de quitter le pays pour relocaliser leur activité ou leurs sièges dans l'Union Européenne, augmenterait alors le risque de pertes ou fuites de données. Les phases de licenciements et de réorganisations industrielles semblent en effet propices à de tels phénomènes[5].

Pour l'heure les entreprises ne paraissent pas avoir engagé de mouvement massif de délocalisation, relocalisation de leurs activités vers l'UE. Début juillet 2016 l'entreprise américaine KKR confirmait même sa décision d'investissement de 65 millions de dollars dans Darktrace, entreprise de cybersécurité créée à Cambridge en 2013. Cet investissement serait justifié, selon KKR, par la dimension internationale du marché de Darktrace[6], qui dispose par ailleurs d'implantations dans plusieurs pays.

Un haut fonctionnaire allemand rappelait récemment qu'en matière numérique, l'UE est fragmentée, composée de 28 (désormais 27) marchés distincts[7]. Le Royaume-Uni pourra donc continuer de prospecter les Etats européens individuellement à la recherche de marchés nationaux. La politique mise en place par les autorités britanniques depuis 2013, d'aide à l'exportation pour les entreprises de cybersécurité[8], se fixe pour objectif d'atteindre un chiffre d'affaire de 2 milliards de livres en 2016 et 4 milliards en 2020[9]. Les priorités géographiques définies dans le plan duUKTI (United Kingdom Trade & Investment) ne sont d'autre part pas européennes :

- les principaux marchés en 2011 étaient aux USA (31%), en Chine -19%), au Japon (10%), l'Inde s'inscrivant comme un marché d'avenir[10]
- la stratégie d'exportation se focalisera sur les Etats du Golfe (où la France, l'Allemagne et les Etats-Unis demeurent les principaux concurrents du Royaume-Uni), le Brésil, l'Inde, la Malaisie[11]
- sont considérés comme marchés déjà matures et de niche, les pays suivants : USA, Canada, Nouvelle Zélande, Australie, Japon, Chine, France, Allemagne, Pays-Bas, pays nordiques.

---

[4] Agamoni Ghosh, India Ashok, "How will Brexit affect cybersecurity in the UK? What the experts are saying about leaving the EU", 23 juin 2016, site International Business Times, http://www.ibtimes.co.uk/how-will-brexit-affect-cybersecurity-uk-what-experts-are-saying-about-leaving-eu-1567008

[5] Pierluigi Paganini, "Brexit's effects on cyber security", 7 juillet 2016, http://resources.infosecinstitute.com/brexit-effects-on-cyber-security/

[6] Simon Clark, «Despite Brexit, KKR Buys Stake in U.K. Cybersecurity Company", The Wall Street Journal, 6 juillet 2016, UK, http://www.wsj.com/articles/despite-brexit-kkr-buys-stake-in-u-k-cybersecurity-company-1467830534

[7] Marco Mayer, Luigi Matino, "Cyber Defense and Cyber Security Policies in the UK and Germany », 5-6 mai 2015, 32 pages, http://www.rise.unifi.it/upload/sub/eu-conference--may-6_mayer.pdf

[8] UK Trade & Investment, "Cyber Security. The UK's approach to exports", avril 2013, UK, 24 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

[9] Cabinet Office, « 2010 to 2015 government policy : cyber security », Policy Paper, 8 mai 2015, Londres, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-6-promoting-economic-growth-in-the-cyber-security-sector

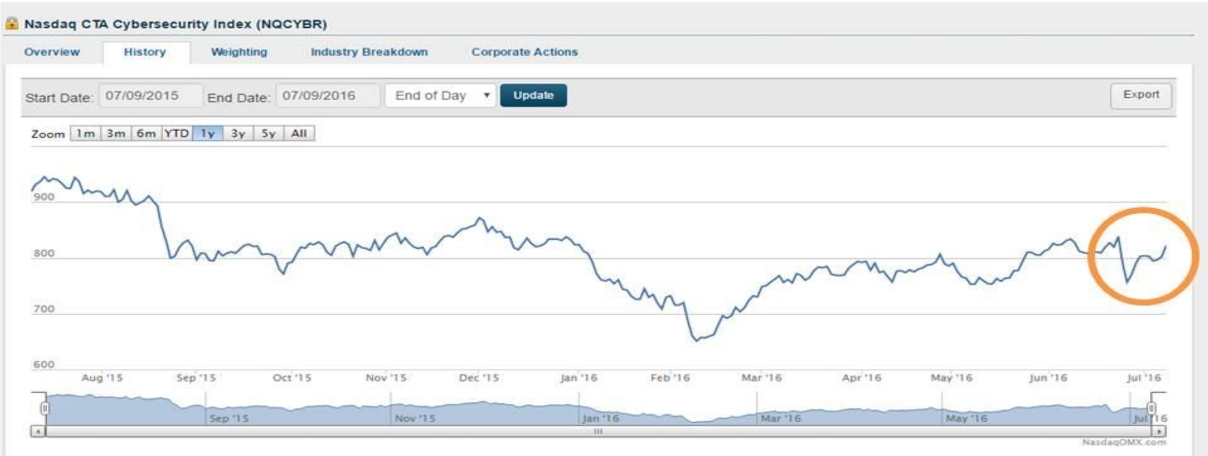
[10] UK Trade & Investment, "Cyber Security. The UK's approach to exports", avril 2013, UK, 24 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

[11] page 14 et suiv. du rapport : UK Trade & Investment, "Cyber Security. The UK's approach to exports", avril 2013, UK, 24 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

- des actions spécifiques seront ciblées sur ce que le rapport désigne « groupes non géographiques », à savoir l'OTAN, l'UE et les Nations Unies.

La stratégie commerciale du Royaume-Uni n'est donc pas axée sur l'UE si l'on s'en réfère à cette source. Elle serait essentiellement tournée vers les Etats-Unis, lesquels demeurent le principal investisseur dans le pays[12].

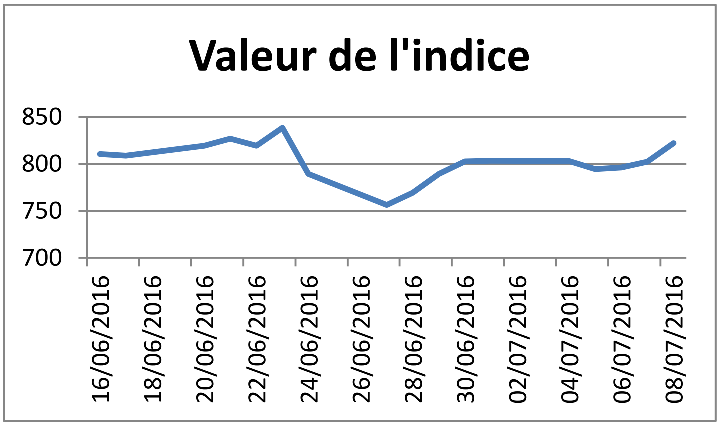
Les effets du Brexit pourront être visibles sur la capitalisation boursière des entreprises de cybersécurité britanniques.



Courbe de l'indice Nasdaq CTA Cybersecurity (NQCYBR) du 9 juillet 2015 au 9 juillet 2016.

L'indice CQCYBR (Nasdaq) a subi une baisse relativement faible et de courte durée suite au référendum sur le Brexit. La réaction est notable dès le 24 juin 2016 par une baisse de l'indice mais il renoue avec une tendance haussière dès le 28 juin 2016. L'indice n'a pas décroché et demeure dans ses valeurs moyennes. Les évolutions des indices au cours des prochains mois pourront d'autre part avoir bien d'autres causes que le seul Brexit.

[12] page 15 du rapport : HM Government, "A strong Britain in an age of uncertainty: the national security strategy", octobre 2010, 39 pages, Londres, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf



Evolution de l'indice CQCYBR du 16 juin au 9 juillet 2016

Nous retrouvons cette même courbe[13] sur le site de l'ISE Cyber Security® UCITS Index[14]. En annexe de cet article nous fournissons une liste indicative des principales entreprises britanniques de cybersécurité, dont l'avenir face au Brexit pourra être observé plus attentivement dans les prochains mois.

1.2. Le coût de la lutte contre la cybercriminalité

La cybercriminalité aura pu se saisir de l'événement que constitue le Brexit : des hackers ont utilisé le terme « Brexit » pour leurs campagnes de spamming ou de phishing[15]. Mais au-delà de ce phénomène ponctuel, des perturbations structurelles, plus profondes, dans l'organisation des institutions et moyens de lutte contre la cybercriminalité, pourraient avoir un impact sur la cybersécurité. Le nouveau gouvernement va-t-il remettre en question l'architecture de cybersécurité étatique construite au cours des années passées ? Cela paraît peu probable à court terme. D'autres facteurs pourraient avoir des conséquences plus immédiates : la baisse de la monnaie britannique pourrait par exemple accroître le coût d'acquisition des solutions de cybersécurité.

(baisse de la Livre Sterling → hausse coût des produits de cybersécurité → baisse des acquisitions de produits de cybersécurité → vulnérabilité accrue des systèmes des entreprises et de l'Etat)
+
(remise en question du partage d'information avec pays UE en matière de cybercriminalité → moins d'efficacité dans la lutte contre la cybermenace)
=
Hausse de la cybercriminalité au Royaume-Uni

Illustration : Quelques effets négatifs du Brexit sur la cybersécurité, du point de vue des anti-Brexit

2 – Politiques, stratégies : sécurité nationale et cybersécurité

2.1. L'interaction entre niveau national et international

Les partisans du Brexit sont convaincus de l'absence d'effet négatif sur la sécurité nationale, en raison du prima de la relation à l'OTAN d'une part pour les questions de défense[16], et d'autre part de

[13] http://www.ise.com/HUR
[14] ISE – ETF Ventures, « Cyber Security », 2 pages, http://www.ise.com/assets/files/index/ETF_HUR_CyberSecurity_0216.pdf
[15] Chris Baraniuk, « Spike in Brexit email spam following referendum result", BBC News, 5 juillet 2016, http://www.bbc.com/news/technology-36714384
[16] « *The fact is that our security depends on NATO, not the EU, and if we leave the EU, we will be just as safe as we are now."* (Sir Edward Leigh (Gainsborough) (Con). Citation extradite de : "EU Withdrawal: effect on

la supériorité des initiatives nationales sur le niveau européen en matière de police et de justice par exemple[17]. Selon eux, être à l'intérieur ou à l'extérieur de l'UE ne changerait rien, parce que le niveau européen n'est définitivement pas celui où la sécurité se joue. D'autres ont une analyse radicalement différente, estimant que l'appartenance à l'UE est vitale pour la sécurité[18], car l'UE permet d'affronter les problématiques globales que les Etats seuls ne peuvent traiter.
Si, effectivement, les politiques et stratégies de cybersécurité des Etats membres relèvent en priorité d'initiatives nationales[19], les niveaux européen et international n'en viennent pas moins interférer avec celles-ci.
La stratégie de sécurité nationale (publiée en 2010)[20] conditionne ainsi la sécurité et la défense du Royaume-Uni à **l'existence de ses relations privilégiées avec les Etats-Unis**, à son appartenance à l'Union Européenne ainsi qu'à l'OTAN ou encore au Conseil de Sécurité. L'alliance avec les Etats-Unis y est qualifiée d'alliance « clef », et **la présence au sein de l'UE de « partenariat vital ».**
La stratégie de cybersécurité de 2011[21] inscrit la **coopération internationale** au rang des moyens de lutte contre la cybercriminalité. Elle prévoit entre autre l'application de la convention de Budapest, de la directive européenne relative aux attaques contre les systèmes d'information, de la directive européenne sur la protection des données.
Le rapport d'avancement de la mise en œuvre de la stratégie de cybersécurité, publié en 2014[22], fait état de la contribution significative du Royaume-Uni dans la formulation d'une stratégie européenne de cybersécurité : « **Le Royaume-Uni a soutenu avec succès la mise en forme de la stratégie de**

---

national security", 18 avril 2016, https://hansard.parliament.uk/Commons/2016-04-18/debates/1604186000015/EUWithdrawalEffectOnNationalSecurity#contribution-1604186000098

[17] « *National military and police intelligence networks are not dependent on the EU, though they may be enhanced by the EU, such as through* Europol. *Cooperation with other European security institutions is not determined by membership of the EU. […] Being in or out may have major effects on many areas of life, but national security is unlikely to be one of them, at least in the short term*." Professor David Galbreath, Professor of International Security, Associate Dean (Research). Citation extradite de : "Professor David Galbreath on: Security in, secure out: Brexit's impact on security and defence policy", 24 mars 2016, http://blogs.bath.ac.uk/iprblog/2016/03/24/professor-david-galbreath-on-security-in-secure-out-brexits-impact-on-security-and-defence-policy/

[18] "*In the areas of serious organised crime, counter-terrorism, money laundering and drugs and people trafficking, there is hugely fruitful EU-wide cooperation recognising the cross-border nature of the threats*". Citation extradite de : Mark Field, "Mark Field: Remaining in the EU is vital to our national security", site conservativehome.com, 27 janvier 2016, http://www.conservativehome.com/platform/2016/01/mark-field-remaining-in-the-eu-is-vital-to-our-national-security.html

[19] Une étude de l'ENISA relative au partage d'information de cybersécurité, publiée en décembre 2015, relève essentiellement les pratiques d'échange à l'intérieur même des Etats, entre institutions collectant de la donnée de cybersécurité, sur les menaces, risques, attaques, croisant les approches sectorielles, favorisant le partage d'informations public-privé. L'étude ne dit rien des pratiques de partage d'information au sein même de l'Union Européenne. ENISA, « Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches", décembre 2015, 64 pages, Grèce, https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

[20] HM Government, "A strong Britain in an age of uncertainty: the national security strategy", octobre 2010, 39 pages, Londres, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[21] Cabinet Office, "The UK cyber security strategy. Protecting and promoting the Uk in a digital world", novembre 2011, Londres, 43 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[22] Cabinet Office, "The UK cyber security strategy. Report on Progress and forward plans", décembre 2014, 24 pages, Londres, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

cybersécurité de l'UE, fournissant une base plus solide pour la coopération avec les autres états membres de l'UE »[23].

Le Brexit aura pour **effet d'éloigner le Royaume-Uni de ce partenariat jugé jusqu'alors vital.** Il n'aura en principe plus accès aux exercices de cybersécurité menés en Europe (comme par exemple l'exercice Cyber Europe qui entraîne les Etats membres à coopérer en cas de crise cyber**). Il lui faudra donc privilégier le mode de relation bilatéral[24],** qui prévaut d'ailleurs déjà en matière de cybersécurité entre les Etats, de façon générale, et s'appuyer sur ses **relations spécifiques avec les Etats-Unis** (sur le modèle de ce qui se pratique déjà, en matière de cybersécurité[25] et de cyberdéfense[26], et de renseignement entre la NSA, le FBI et le GCHQ ou le MI5)[27]. Selon Tim Edgar, chercheur au Brown University's Watson Institute, le retrait du Royaume-Uni signifie cependant la perte, pour les Etats-Unis, d'un allié proche et puissant au sein de l'UE, notamment sur les questions de renseignement, de cybersécurité et de contre-terrorisme[28]. Ce retrait pourrait selon lui avoir des impacts à long terme sur les alliances entre les Etats-Unis et de nombreux pays du monde.

Pour partager de l'information de cybersécurité et cyberdéfense avec l'UE, le Royaume-Uni pourra peut-être compter sur sa présence au sein de l'OTAN. En février 2016, l'OTAN et l'UE ont signé un accord[29] facilitant le partage d'information technique entre le NATO Computer Incident Response Capability (NCIRC) et le Computer Emergency Response Team - European Union (CERT-EU). Le Royaume-Uni devra également reconsidérer la participation qu'il avait jusqu'ici au sein d'Europol et du Centre Européen de Cybercriminalité (EC3)[30], organisations européennes de lutte contre la cybercriminalité[31].

En se retirant rapidement de l'UE, le Royaume-Uni n'aura pas à transposer dans son droit national la nouvelle directive NIS (Directive on security of network and information systems) adoptée par le Parlement européen le 6 juillet 2016 (et devant entrer en application en août 2016), qui vise à

---

[23] Page 16 du rapport.

[24] Pour les pays européens, les effets du Brexit s'apprécieront aussi de manière individuelle, l'intensité des relations avec le Royaume-Uni variant fortement d'un Etat membre à un autre. Une étude réalisée par Global Counsel en juin 2015, tentait d'apprécier le degré d'exposition de chaque Etat membre aux effets négatifs du Brexit (notons que ce rapport ne fait jamais mention de la cybersécurité). Les Pays-Bas, l'Irlande et Chypre constituaient alors le trio de tête des pays les plus exposés. Venait ensuite un groupe de pays exposés de manière significative, puis un groupe caractérisé par des expositions ponctuelles (, pays) dans lequel on retrouve la France et l'Estonie ; enfin un dernier groupe à faible exposition. La métrique utilisée s'appuie sur des variables économiques et financières essentiellement. Global Counsel, « Brexit : the impact on the Uk and the EU", Juin 2015, 44 pages, https://www.global-counsel.co.uk/sites/default/files/special-reports/downloads/Global%20Counsel_Impact_of_Brexit.pdf

[25] - Robert Hutton, "UK. and U.S. banks plan joint cyber security attack test", 16 janvier 2015, http://www.bloomberg.com/news/articles/2015-01-16/u-k-and-u-s-banks-plan-joint-cyber-security-attack-test
- "US, UK plan cyber 'war games' to boost defense against hackers", site RT.com, 16 janvier 2015, https://www.rt.com/usa/223175-usa-uk-cyber-war-games/

[26] Voir le annexes 3 et 4 du document suivant : Cabinet Office, « 2010 to 2015 government policy : cyber security », Policy Paper, 8 mai 2015, Londres, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-6-promoting-economic-growth-in-the-cyber-security-sector

[27] The White House, « US – United Kingdom cybersecurity cooperation", 16 janvier 2015, Etats-Unis, https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation

[28] Watson Institute for International and Public Affairs, « Tim Edgar explains the security implications surrounding the Brexit vote", video, https://www.youtube.com/watch?v=nCtDNEdEAdc

[29] Press Release, « EU and NATO increase information sharing on cyber incidents", 10 février 2016, Bruxelles, http://www.eeas.europa.eu/statements-eeas/2016/160210_01_en_en.htm

[30] European Cybercrime Centre

[31] http://resources.infosecinstitute.com/brexit-effects-on-cyber-security/

homogénéiser les capacités de cybersécurité des Etats membres[32] et à forger un cadre pour l'échange d'informations (les Etats membres disposent quant à eux de 21 mois pour transposer la directive dans leur droit national)[33]. Mais il devra se conformer à la nouvelle régulation européenne sur les données, la General Data Protection Regulation "GDPR" (règle qui devra s'appliquer à toutes les entreprises dans le monde, qui traiteront des données des citoyens européens).
Les changements induits par le Brexit s'apprécieront dans la manière dont le Royaume-Uni se positionnera sur les questions relatives à la protection des données, de la vie privée, à la cybercriminalité[34] ou encore à la cybersurveillance.

2.2. Le nouveau gouvernement

La nomination d'un nouveau premier ministre aura très certainement des conséquences sur les choix politiques et stratégiques en matière de cybersécurité. Mme Theresa May, qui a pris ses fonctions de 1° Ministre le 13 juillet 2016, est partisane de choix radicaux, car selon elle vouloir établir et maintenir un équilibre entre le droit à la vie privée et la sécurité est impossible[35]. Priorité doit donc être donnée à la sécurité, et ce faisant tous les moyens d'action nécessaires attribués aux acteurs de la sécurité. La loi qui concrétise cette vision, Loi sur les compétences de l'instruction surnommée IP Bill ("loi IP"), a été adoptée en mars 2016 par le Parlement britannique. On dit donc de Theresa May qu'elle a été le promoteur de la loi sur la cybersurveillance britannique. La politique de cybersécurité du Royaume-Uni, durant la phase du Brexit, sera celle du parti conservateur, dont les grandes lignes sont les suivantes[36] :

- maintien des moyens alloués à la lutte contre la cybercriminalité, développement de la cyber-police, et recours à des réservistes, volontaires, pour seconder les forces de police (les « cyber specials » ou « iPlods »)
- maintien des investissements en cyberdéfense pour construire des armées flexibles, modernes
- renforcement des moyens de lutte contre le terrorisme sur internet, appelant à un développement des pratiques et moyens de cybersurveillance
- faire du Sud-Ouest du Royaume-Uni un centre d'excellence en cybersécurité (et plus généralement affaires militaires).
- création de nouveaux hubs de R&D

[32] L'association BSA publiait en 2015 une étude comparant le niveau de maturité en cybersécurité des pays de l'UE, appuyant cette comparaison sur un ensemble de critères (toujours teinté de subjectivité), tels que les fondements juridiques, l'existence d'entités opérationnelles, de mesures de partenariat public-privé, de plans spécifiques à la cybersécurité, et de formation. 25 items sont considérés. Le Royaume-Uni satisfait 16 de ces items (11 pays répondant à plus de 12 items ; 17 pays à moins de 12 items) et se situe donc plutôt dans la catégorie des bons élèves, aux côtés de l'Autriche, la République Tchèque, l'Estonie, la Finlande, l'Allemagne, l'Italie, la Lettonie, les Pays-Bas, l'Espagne. BSA, « EU cyberecurity dashboard", 2015, Washington, 20 pages, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
[33] "The Directive on security of network and information systems (NIS Directive)", https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[34] David Fidler, "The implications of Brexit on UK cyber policy", 28 juin 2016, site Net Politics, http://blogs.cfr.org/cyber/2016/06/28/the-implications-of-brexit-on-uk-cyber-policy/
[35] « GB: la secrétaire d'État à l'Intérieur favorable à la surveillance des services secrets », 11 juin 2015, https://fr.sputniknews.com/international/201506111016523667/
[36] - "The next five years of Cyber Security", https://www.templarexecs.com/the-next-five-years-of-cyber-security/
- Mike Hine, « UK General Eection 2015: what the major parties promise on security", site infosecurity, article non daté, http://www.infosecurity-magazine.com/news-features/uk-general-election-2015-security/

Pour comparaison, rappelons les priorités définies par les autres partis politiques au Royaume-Uni en matière de cybersécurité[37] :

- tous les partis politiques conviennent, mis à part le parti écologiste, de la nécessité d'investir en cybersécurité et dans la lutte contre la cybercriminalité
- les verts veulent soutenir la politique européenne de protection des données en s'opposant à la privatisation et marchandisation des données personnelles ; ils veulent s'opposer à la cybersurveillance ; ils souhaitent défendre les libertés sur Internet
- les travaillistes souhaitent renforcer les obligations pesant sur les entreprises, les infrastructures critiques, les contraignant à déclarer les cyberattaques subies ; construire la cybersécurité en s'appuyant sur les compétences industrielles du pays ; comme les libéraux-démocrates veulent déployer un internet, des réseaux très haut-débit sur l'ensemble du territoire ; soutenir des clusters de hautes technologies.
- les démocrates libéraux défendent le droit de chacun sur ses propres données ; focalisent leur action sur la question des données personnelles, en accordant aux individus, aux entreprises, aux administrations publiques, le droit de recourir à de la cryptographie forte ; entendent investir dans la cyberdéfense (capacités pour contrer les cyberattaques). Mais si les pratiques de surveillance doivent être strictement encadrées, les libéraux démocrates affichent la volonté de maintenir les investissements dans les agences de sécurité et de renseignement pour contrer les menaces de cyberattaques.

Au Royaume-Uni, la question de la cybersécurité semble faire désormais partie des débats politiques, tous partis confondus. Le sujet s'est politisé, et nul doute que les révélations d'E. Snowden auront joué un rôle essentiel dans cette accélération de l'intégration du cyber aux considérations politiques.

Conclusion

L'expérience du Brexit sera pour l'UE au moins aussi riche d'enseignements que tout processus d'élargissement, révélant notamment sa capacité d'absorption des chocs. S'il a pu être avancé que l'appartenance à l'UE renforce la sécurité intérieure de ses membres (l'UE créerait, apporterait de la sécurité à ses membres)[38] d'autres avis estiment au contraire que l'UE est de peu d'effet sur la sécurité intérieure des Etats membres[39]. Par comparaison entre un avant et un après, le cas du Royaume-Uni sera riche d'enseignements sur ces questions sécuritaires. Un travail sur le long terme mérite d'être engagé dès à présent, afin d'observer les transformations sécuritaires induites par le

[37] Ces constats sont repris d'une courte analyse publiée sur le site ncchroup (« How do the UK's political parties view cyber security? », mai 2015, https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/may/how-do-the-uks-political-parties-view-cyber-security/) et sur le site http://www.infosecurity-magazine.com/news-features/uk-general-election-2015-security/

[38] - Bartosz Sklodowski, « The membership in the EU and the internal security of Poland. Benefits, Costs, Perspectives", 27 pages, http://en.oapuw.pl/wp-content/uploads/2013/03/Sklodkowski-B-The-membership.pdf

- Carmen Stoian, « The Benefits and Limitations of European Union Membership as a Security Mechanism", 29 pages, https://kar.kent.ac.uk/3139/1/paper_jei.pdf

- Márton Csanády, Csaba Törő, « The Effects of EU Membership on Hungarian Foreign and Security Policy Perspectives, Perceptions and Practices – A Brief Impact Assessment", Foreign Policy Review, 2013, 19 pages, http://kki.gov.hu/download/5/3a/c0000/FPR_Beliv_003.pdf

- "Row as ex-intelligence chiefs say EU membership protects UK security", BBC News, 8 mai 2016, http://www.bbc.com/news/uk-36239741

[39] "*The union is not a natural contributor to national security of each of the entity states and in some ways gets in the way of the state providing security for its own citizens*." Citation extraite de l'article: "EU membership 'sometimes gets in the way' of national security, says ex-CIA chief", Heraldscotland.com, 25 mars 2016, http://www.heraldscotland.com/news/14384423.EU_membership__sometimes_gets_in_the_way__of_national_security__says_ex_CIA_chief/?ref=rss

Brexit, pour les trois niveaux que sont la situation du Royaume-Uni, celle de l'UE et celle du reste du monde.
En observant ce que perdront ou gagneront chacun de ces niveaux, nous comprendrons mieux les implications réelles de la construction européenne sur les enjeux de sécurité.
Le Brexit crée un précédent pour l'Union Européenne. Mais il rappelle aussi qu'en matière de relations internationales rien n'est figé. La configuration du monde il y a un siècle était fort différente de l'actuelle, et il est évident que celle de demain diffèrera tout autant. Les constructions politiques, les frontières, les rapports de puissance sont animés de mouvements incessants, dont le Brexit n'est que l'une des manifestations.

ANNEXE : entreprises britanniques de cybersécurité

La liste ci-dessous est extraite, le 11 juillet 2016, de la liste des 500 entreprises de cybersécurité les plus importantes dans le monde, identifiées par le site cybersecurityventures.com
31 entreprises « britanniques » seraient ainsi identifiées.

Rang dans la liste des 500 entreprises	Nom de l'entreprise	Secteur de Cybersécurité	Siège
8	BT	Security & Risk Management Solutions	London, UK
10	Sophos	Anti-Virus & Malware Protection	Abingdon, UK
12	BAE Systems	Cybersecurity Risk Management	Surrey, UK
24	Nexusguard	Cloud Enabled DDoS Mitigation	San Francisco CA
32	PwC	Cybersecurity Consulting & Advisory	London, UK
42	EY	Cybersecurity Advisory Services	London, UK
67	NNT	IT Security & Compliance	St. Albans, UK
87	PKWARE	Data Encryption & Security	Milwaukee WI
89	SentryBay	PC, Mobile & IoT Security	London, UK
95	KPMG	Cyber Risk Management	London, UK
129	NCC Group	Information Assurance Services	Manchester, UK
135	neXus	PKI, Access & Identity Management	Hagersten, Sweden
140	Bromium	Endpoint Security	Cupertino CA
176	Osirium	Privileged User Management	Berkshire, UK
179	Intercede	Mobile Identity Management	Leicestershire, UK
191	Clearswift	Data Loss Prevention	Reading, UK
197	Swivel Secure	Risk Based Authentication	Wetherrby, UK
219	Digital Shadows	Cyber Intelligence Feeds	East Sussex, UK
250	Smoothwall	Unified Threat Management	Leeds, UK
258	Becrypt	Mobile Device & Data Security	London, UK
298	Deep Secure	Content Control & Inspection	Malvern, UK
301	Acuity Risk Management	IT Governance, RIsk & Compliance	London, UK
311	Darktrace	Cyber Threat Prevention	London, UK
314	Avecto	Endpoint Security Software	Cheshire, UK
332	Epsion	IT Governance, Risk & Compliance	Dublin, Ireland
350	Acunetix	Web Vulnerability Scanner	Kingston Upon Thames, UK
354	PortSwigger	Web Application Security Testing	Knutsford, UK
358	Wandera	Secure Mobile Gateway	London, UK
433	QuintiQ	Cyber Consulting & Services	Farnborough, UK
449	Emailage	Fraud Detection & Prevention	Chandler AZ
487	Protectimus	Two Factor Authentication	London, UK

______________________ *Chaire Cyber-Défense et Cyber-sécurité* ____________________________

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires