Can the Brexit have an impact on Cybersecurity in the United Kingdom and elsewhere?

Daniel Ventre, CNRS (CESDIP), Chair-holder of the Chair of Cybersecurity and Cyberdefense

July 15th, 2016, article III – 25
Translated from French

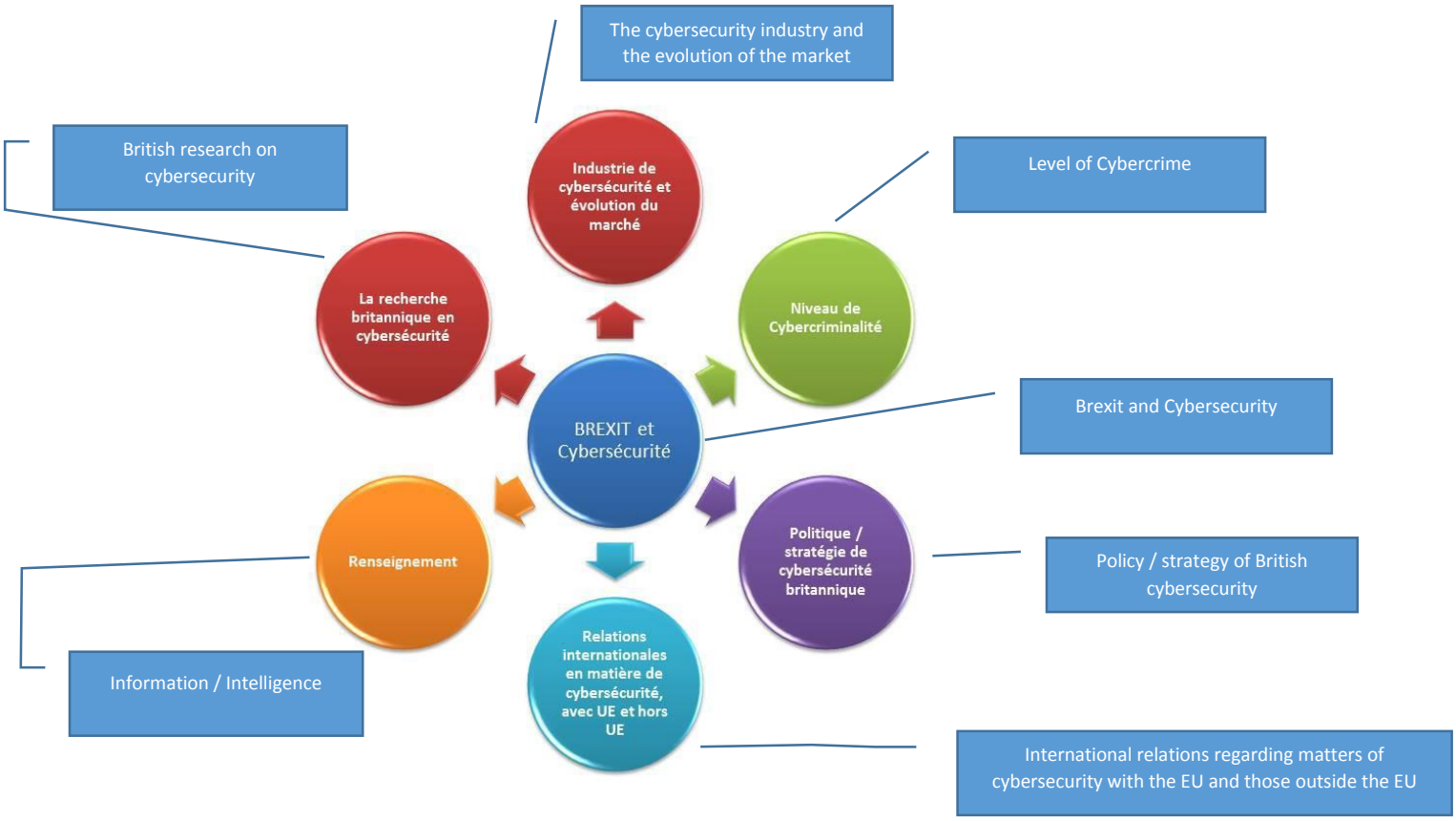
On June 23rd, 2016 the British public was called upon to decide the fate of the presence of the United Kingdom in the European Union. The results of the referendum, announced on June 24th 2016, confirmed the success of the Brexit, with 52% voting to support the exit while 48% voted against it. On July 13th, the Conservative, Theresa May, was appointed Prime Minister. She will take charge of managing the process of the U.K. exiting the European Union. Well before the elections and the results, analysts had attempted to understand the short, medium and long term effects of the Brexit for the U.K., the EU, and the rest of the world in terms of economic, financial, business, social, and immigration concerns.[1]

Among the first effects of the exit that came in anticipation of the results were that stock prices fell, as did the value of the pound, approaching parity with the Euro. Shortly after, Standard & Poor made a decision to downgrade the U.K.'s rating. There also followed a brief period of political uncertainty, where political figures supporting the Brexit refused to take leadership in the government. Now, one must ask what effect this has on security. One of the key arguments of Brexit supporters was precisely that of security. They argued that leaving the EU would allow the U.K. to regain its sovereignty and thus it would be better equipped, hands free, to confront the issue of immigration, and defend its borders and national space. As if to withdraw from the EU would allow the U.K. to protect itself from the problems and effects of globalization.

This paper poses specific questions surrounding the effects of the Brexit on cybersecurity, which elicit mixed responses, positive[2] for some and negative for others.[3] We look at cybersecurity from an economic

[1] Vaughne Miller, "Exiting the EU : impact in key UK policy areas," Briefing Paper, no. 07213, 12 February 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 June 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

point of view (business and the cost to fight cybercrime), and political point of view (the prospects of the new government and the links between national policies and international affairs).



Effects of the Brexit on cybersecurity: a few key points to observe

1 – The Economy

1.1 Private Sector

Like all other economic activities, the cybersecurity industry, is likely undergoing transformations brought on by the Brexit, either because of regulatory changes within the U.K. or because of changes related to the single market. Below are some variables that could likely bring about consequences:

- The private sector has benefited from EU aid, which will no longer be available. Just think of the many grants given by the EU in R&D through the Framework Programmes. The private sector, like the academic research fields, will be lacking these grants and there is no guarantee that the British government knows how to replace these costly resources.
- The private sector benefited from the structure of the single market and the free movement of goods, capital and people. The new restrictions will inhibit freedom of movement, which had formerly helped to drive businesses in terms of human resources (attracting talent), in particular. The restrictions make the U.K. potentially less attractive.

- The attractiveness of the British market and businesses will suffer due to increased costs that will weigh on employment and trade (because of the need for visas for foreigners, taxes, and rising costs of transactions with other European countries, etc.).[4]
- If companies located in the U.K. decide to leave the country to relocate their businesses or their headquarters to the European Union, this would increase the risk of data losses or leakage. These phases of layoffs and reorganization (associated with relocation) may or may not lead to such a phenomenon.[5]

For now companies do not appear to be moving in mass to relocate their activities to the EU. At the beginning of July 2016, the U.S. company KKR confirmed its decision to invest 65 million dollars in Darktrace, a cybersecurity company founded in Cambridge in 2013. This investment is justified, according to KKR, because of the international dimension of Darktrace,[6] which has offices in several countries.

A senior German official recently noted that, in terms of the digital domain, the EU is fragmented, with 28 (now 27) distinct markets.[7] The U.K. will therefore continue to explore European countries individually, searching for national markets. The policy implemented by British authorities in 2013 to aid cybersecurity[8] companies to export their products, has the goal of achieving a turnover of 2 billion pounds in 2016 and 4 billion pounds in 2020.[9] The geographic priorities defined in the UKTI (United Kingdom Trade & Investment) plan are not European:

- The major markets in 2011 were the U.S. (31%), China (19%), Japan (10%), and India was listed as an up-and-coming market.[10]
- The export strategy will focus on: the Gulf States (where France, Germany and the United States are still the U.K.'s the main competitors), Brazil, India, and Malaysia.[11]
- The following countries are considered already mature and niche markets: U.S., Canada, New Zealand, Australia, Japan, China, France, Germany, Netherlands, and the Nordic countries.
- Specific actions will be taken on what the report calls "non-geographical groups", ie NATO, the EU and the UN.

The United Kingdom's commercial strategy is not centered on the EU if one refers to the above report. It would be mainly oriented towards the US, which remains the main investor in the country.[12]

---

[4] Agamoni Ghosh, India Ashok, "How will Brexit affect cybersecurity in the UK? What the experts are saying about leaving the EU," 23 June 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 July 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 July 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 May 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," April 2013, UK, 24 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

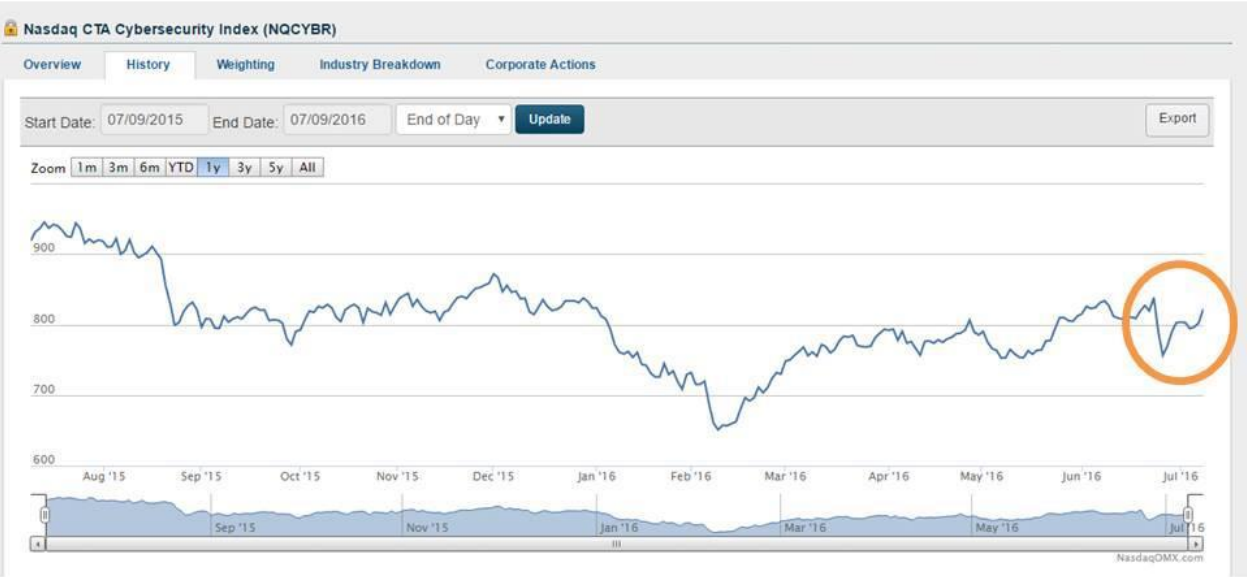
[9] Cabinet Office, "2010 to 2015 government policy : cyber security," Policy Paper, 8 May 2015, London, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-6-promoting-economic-growth-in-the-cyber-security-sector

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

[11] Page 14 and throughout report: UK Trade & Investment, "Cyber Security. The UK's approach to exports," April 2013, UK, 24 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

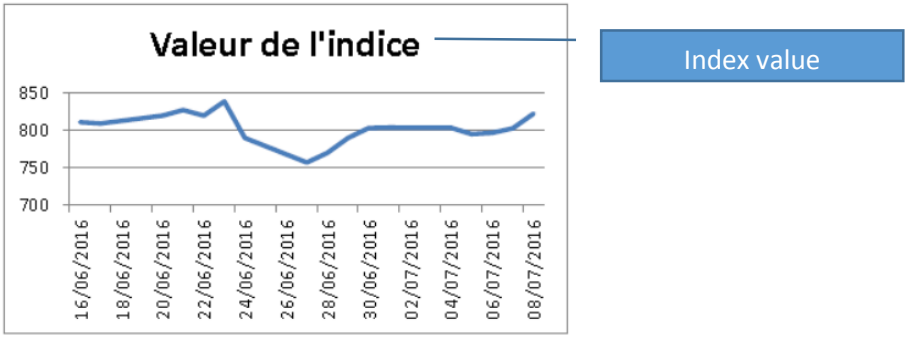
[12] Page 15 of report : HM Government, "A strong Britain in an age of uncertainty: the national security strategy," October 2010, 39 pages, London, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

The effects of the Brexit will be noticeable in regards to the market capitalization of British cybersecurity companies.



Curve of the Nasdaq CTA Cybersecurity Index (NQCYBR) from July 9th, 2015 to July 9th, 2016.

The CQCYBR index (Nasdaq) suffered a relatively small and short decline following the Brexit referendum. One notable market reaction was from June 24th, 2016, which saw a decline in the index but then there is an uptrend starting on June 28th, 2016. Overall, the index has not fallen and remains in an average value range. Changes in the indices in the coming months may be due to things outside of just the Brexit.



Evolution of the CQCYBR Index from June 16 to July 9th, 2016

We find this same curve[13] on the site of the ISE Cyber Security® UCITS Index.[14] In the appendix of this article we provide an indicative list of the U.K.'s cybersecurity companies, whose future facing the Brexit, can be observed more closely in the coming months.

[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

1.2 The cost of the fight against cybercrime

Cybercriminals have been able to take advantage of the events surrounding the Brexit. Hackers used the term "Brexit" for their spamming and phishing campaigns.[15] However, beyond this specific phenomenon, there are deeper structural issues in the organization of institutions and methods of fighting against cybercrime that could have an impact on cybersecurity. Will the new government question the existing cybersecurity architecture that has been constructed over the course of many years? This seems unlikely in the short-term. Other factors could have more immediate consequences, such as the decline of British currency that could, for example, increase the acquisition cost of cybersecurity solutions.

(Devaluation of the pound → rise in the cost of cybersecurity products → decrease in the acquisition of cybersecurity products → increased vulnerability of corporate and state systems)
+
(questioning of sharing information with other EU countries on cybercrime → less efficiency in the fight against cyberthreats)
=
Rise of cybercrime in the U.K.

Illustration: A few negative effects of the Brexit on cybersecurity from an anti-Brexit point of view

2 – Policies and strategies: National security and cybersecurity
2.1 Interaction between the national and international levels

Many Brexit supporters are convinced that the exit will have no negative effects on national security because of Britain's privileged relationship with NATO for defense,[16] and also because they believe national initiatives on policing and justice to be superior to the European ones.[17] According to them, being inside or outside the EU would not make a difference, because they believe that security issues are not played out on the European level. Others have a radically different analysis, arguing that membership in the EU is vital for safety[18] because the EU can address global issues that states cannot tackle alone. Even if

[15] Chris Baraniuk, "Spike in Brexit email spam following referendum result," BBC News, 5 July 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 extracted from: "EU Withdrawal: effect on national security," 18 April 2016, https://hansard.parliament.uk/Commons/2016-04-18/debates/16041860000015/EUWithdrawalEffectOnNationalSecurity#contribution-16041860000098

[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 extracted from: "Professor David Galbreath on: Security in, secure out: Brexit's impact on security and defence policy," 24 March 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 extracted from: Mark Field, "Mark Field: Remaining in the EU is vital to our national security," site conservativehome.com, 27 January 2016, http://www.conservativehome.com/platform/2016/01/mark-field-remaining-in-the-eu-is-vital-to-our-national-security.html

Member States prioritize their political and cybersecurity strategies of national initiatives,[19] the European and international levels do, nevertheless, interfere with them.

The National Security Strategy (published in 2010),[20] defines the security and defense strategies of the U.K. from **the existence of its privileged relations with the United States** to its membership in the EU, as well as NATO, and the Security Council. The alliance with the U.S. is qualified as a "key" alliance and it describes **its presence in the EU as a "vital partnership."** The U.K. Cyber Security Strategy[21] report published in 2011 cited **international cooperation** among the ways to fight cybercrime. It covers, among other things, the implementation of the Budapest Convention, the European Directive on attacks against information systems, and the European Directive on data protection. The UK Cyber Security Strategy Report on Progress and Forward Plans, published in 2014,[22] acknowledges the significant contribution the U.K. has made in the creation of the European cybersecurity strategy. "**The U.K. successfully helped shape the EU cyber security strategy**, providing a stronger basis for co-operation with other EU Member States."[23]

The Brexit will **effectively remove the U.K. from this partnership that was deemed vital until now**. The U.K., in principle, will no longer have access to the cybersecurity exercises conducted in Europe (such as the Cyber Europe exercise that trains Member States on how to cooperate in case of a cyber-crisis). The U.K. will therefore **have to prioritize bilateral relationships**,[24] which often exist in the field of cybersecurity between states. Generally speaking, it could rely on its special relationship with the United States, using the models already in place regarding cybersecurity[25] and cyberdefense,[26] and also regarding information sharing between the NSA, FBI and GCHQ or MI5.[27] According to Tim Edgar, researcher at Brown University's Watson Institute, the U.K.'s withdrawal represents a loss for the United States, which will lose a powerful and close ally within the EU, notably on issues such as intelligence, cybersecurity and counterterrorism.[28] The withdrawal could, according to him, have a long-term impact on alliances with the United States and numerous other countries. In order to share information with the EU on cybersecurity

---

[19] A study by ENISA on the sharing of cybersecurity information, published in December 2015, essentially covers exchange practices within states, between cybersecurity institutions collecting data on threats, risks, attacks, intersecting sectors, promoting the sharing of private-public information. The study says nothing about the information sharing practices within the European Union. ENISA, "Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches," December 2015, 64 pages, Greece, https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

[20] HM Government, "A strong Britain in an age of uncertainty: the national security strategy," October 2010, 39 pages, London, 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," November 2011, London, 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," December 2014, 24 pages, London, 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

[23] Page 16 of report

[24] The Brexit will have an effect on European countries individually, for example the degree of relations with the UK will vary greatly from one Member State to another. A study by the Global Counsel in June 2015, attempted to assess the degree of exposure of each Member State to the negative effects of Brexit (note that this report does not mention cybersecurity). The Netherlands, Ireland and Cyprus were the top three countries most exposed. After came a group of countries facing significant exposure, then a group characterized by occasional incidences of exposure, such as France and Estonia. The last group had low exposure. The metrics used are based mainly on economic and financial variables.
Global Counsel, "Brexit : the impact on the Uk and the EU," June 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 January 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 January 2015, https://www.rt.com/usa/223175-usa-uk-cyber-war-games/

[26] See Annexes 3 and 4 of the following document: Cabinet Office, "2010 to 2015 government policy : cyber security," Policy Paper, 8 May 2015, London, 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 January 2015, United States of America, 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

and cyberdefense, perhaps the U.K. will have to rely on its presence within NATO. In February of 2016, NATO and the EU signed an agreement[29] facilitating the sharing of technical information between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team - European Union (CERT-EU). The U.K. will also have to reconsider its participation, up until now, in Europol and the European Cybercrime Centre (EC3),[30] both European organizations that work to fight cybercrime.[31]

By rapidly withdrawing from the EU, the U.K. will not have to legislate the new NIS directive (Directive on security of network and information systems) adopted by the European Parliament on July 6th, 2016, which goes into force in August of 2016. It aims to ensure a high common level of cybersecurity capabilities of Member States[32] and to create a framework for information exchange (Member States have 21 months to transpose the Directive into their national laws).[33] However the U.K. must comply with the new European regulation on data, the General Data Protection Regulation (GDPR), a regulation that must apply to companies worldwide that deal with the data of European citizens. The changes brought about by the Brexit will shape how the U.K. will position itself regarding issues related of data protection, privacy, cybercrime[34] and even cybersurveillance.

2.2 The new government

The appointment of a new prime minister will certainly have consequences on policy and strategic choices in terms of cybersecurity. Theresa May, who took office as Prime Minister on July 13th, 2016, is from a party with extreme views, because according to her, establishing and maintaining a balance between the right to privacy and security is impossible.[35] Priority, therefore, must be given to security and all actions should be taken to give security actors the needed resources. The law in which this vision is manifested, the Investigatory Powers Bill (the IP Bill) was adopted in March 2016 by the British Parliament. Therefore it can be said that Theresa May is a promoter of the British cybersurveillance law. U.K. Cybersecurity policy during the Brexit phase will be that of the Conservative Party, which is guided by some main themes that are listed below: [36]

- maintain the resources allocated to the fight against cybercrime, development of cyber-police and use of reserves, volunteers to assist the police (the "cyber specials" or "iPlods")
- maintain investment in cyberdefense to build modern flexible armies

[29] Press Release, "EU and NATO increase information sharing on cyber incidents," 10 February 2016, Brussels, 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/
[32] In 2015 the BSA association published a study comparing the levels of maturity of cybersecurity of EU countries, this comparison was based on a set of criteria (with a degree of subjectivity) as a legal basis for the existence of operational entities, public-private partnership measures, specific plans for cybersecurity, and trainings. Twenty-five points are considered. The U.K. has fulfilled sixteen of these points (eleven countries meet over twelve points, seventeen countries within twelve points) and they therefore fall into the category of "good students," alongside Austria, the Czech Republic, Estonia, Finland, Germany, Italy, Latvia, the Netherlands, and Spain.
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 June 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 June 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 no date, http://www.infosecurity-magazine.com/news-features/uk-general-election-2015-security/

- reinforce capacity in the fight against terrorism on the internet, calling for the development of practices and methods for cybersurveillance
- make a center of excellence for cybersecurity (and other military affairs) in the southwest of the U.K.
- create new R&D hubs

For the purposes of comparison, below are the priorities defined by the other political parties in the U.K. regarding cybersecurity: [37]

- all political parties agree, except for the Green Party, on the need to invest in cybersecurity and the fight against cybercrime
- the Green Party wants to support the European policy of data protection by opposing the privatization and commodification of personal data, they oppose the proposed cybersurveillance plans, and want to defend internet freedoms
- the Labour Party wants to: reinforce obligations imposed on businesses and their critical infrastructure, requiring them to declare when they have experienced cyberattacks; buildup cybersecurity through the use of the country's commercial competencies; like the Liberal Democrats, they want to deploy high-speed internet networks throughout the country; support clusters of advanced technology.
- Liberal Democrats: support the right of individuals to their own data; focus their actions on issues of personal data, maintaining that individuals, companies, and governments, have the right to the use of advanced cryptography; plan to invest in cyberdefense capabilities to counter cyberattacks. However, if the surveillance laws must be strictly enforced, the Liberal Democrats show willingness to invest in security and intelligence agencies in order to counter the threat of cyberattacks.

In the U.K., the issue of cybersecurity appears to have become a part of political debate by all parties. The subject has become politicized and there is no doubt that the Edward Snowden revelations played a vital role in accelerating the integration of cyber issues into political discourse.

Conclusion

The Brexit will be, at the very least, a rich learning experience for the EU, as instructive as any expansion process, and will notably reveal its capacity to absorb shocks. It has been argued that EU membership strengthens the internal security of its members (as the EU creates and brings security to its members),[38] while others argue that the EU has little influence on the internal security of its Member States.[39] By

[37] These findings are taken from a short analysis published on the site ncchroup "How do the UK's political parties view cyber security?," May 2015, https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/may/how-do-the-uks-political-parties-view-cyber-security/) et and on the 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 May 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 taken from the article: "EU membership 'sometimes gets in the way' of national security, says ex-CIA chief," Heraldscotland.com, 25 March 2016, http://www.heraldscotland.com/news/14384423.EU_membership__sometimes_gets_in_the_way__of_national_security__says_ex_CIA_chief/?ref=rss

comparing the situation before and after the Brexit, the case of the U.K. is rich in lessons regarding security questions. A long-term effort should be committed to now, to observe the security changes brought about by the Brexit on three levels: within the U.K., the EU, and the rest of world. By looking at what is won or lost at each of these levels, we can better understand the real implications of European integration on security issues. The Brexit set a precedent in the EU, and it serves to remind us that international relations are not fixed. A century ago, world order was very different from today, and it is clear that tomorrow it will differ as well. Political structures, borders, and power relations are constantly changing and the Brexit is simply one example of that.

APPENDIX: British cybersecurity firms

On July 11th 2016, the list below was taken from the list of the 500 most important cybersecurity companies in the world, identified by the site cybersecurityventures.com. Thirty-one "British" companies were identified among them.

Rank in the list of 500 companies	Name of firm	Cybersecurity sector	Headquarters
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	Wetherby, 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 (Chair of Cyberdefense and Cybersecurity)
Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Phone number: 01-45-55-43-56 - email: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

The Chair thanks its partners