Cybercrime and Cyber Security and the Legislative Complience in Transitional Countries Compared to EU and China

Elena Tilovska-Kechedji*

Abstract

With the expend of internet, online networks and technology in all spheres of life and the dependence on it, so did cybercrime begun to rise. Countries, institutions, companies are all fearing this new threat. Therefore the actors, policy makers and policies, compliance regulations that are created need to consider all the threats from cyber crime and take actions in regards to cybersecurity. Therefore, in this research we will consider what cyber security measures and legislative compliance's are taken by transitional countries in comparison to EU and China and whether they are enough or there are needed more changes in future.

Keywords: *cybercrime, cyber security, transitional countries, EU and China*

I. Introduction

Today, there are 4.66 billion people or 59.9 % internet users in the world[1] and in 2011, there were around 2.3 billion people in the world, who had access to the internet, so the numbers have increased more than double. In this world of connectivity and increase in the use of technology we have to acknowledge that the crime will not be conducted in the old fashion way, but it will be digitalized as well[2]. The high connectivity is very important for the global development, but it is also important to be protected while conducting the online activities and sharing confidential data which means that there should be increase in the cyber protection. According to the ITU Connect, it is estimated that there will be 70 % Internet breaches by 2023, especially theft of personal data and specific infrastructure breaches. Also, there is a huge gap between countries in terms of implementation of legislation, adoption of national cybersecurity strategies (NCS), and creation of computer emergency response

* Associate professor, Vice Dean for International Cooperation and Science, Faculty of Law, University "St. Kliment Ohridski" – Bitola. Contact: elena-tilovska-kechegi@hotmail.com.

[1] "Global digital population as of January 2021", https://www.statista.com/statistics/617136/digital-population-worldwide/.

[2] Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, Vienna 2013, retrieved from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJEG.4_2013/CYBERCRIME_STUDY_210213.pdf.

teams (CERTs), the same applies to the awareness, capacity and capabilities of governments and companies[3].

In order to begin in depth with discussing the cybercrime and cybersecurity in different countries first we should clarify the terms.

"Cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[4]. Furthermore, "cybercrime is an 'umbrella' term for lots of different types of crimes which either take place online or where technology is a means and/or target for the attack. It is one of the fastest growing criminal activities across the world and can affect both individuals and businesses"[5].

This is a term that describes criminal activities in which computers or computer networks are a tool, a target, or a place of criminal activity. It is an advanced mean used in traditional crimes. For example, the cybercrime can stop railways, it may misguide planes, it can cause military data to fall in the wrong hands, it can make any system to collapse[6].

It is also an issue that does not stop at the border, it can go over it without being detected and it can be classified in three definitions:

- crimes specific to the internet – attacks against information systems, for example: creating fake bank websites to use passwords to access bank accounts;
- online fraud and forgery – on line fraud, for example: identity theft, phishing, spam and using malicious code;
- illegal online content – *like* child sexual abuse material, racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia, trafficking in human beings, drugs trafficking[7].

Furthermore, Cyber security is the preventive application of technologies, processes, legislation and controls to protect the systems, the networks, programs, devices and data from cyber attacks. It aims to reduce the risk of this kind of attacks and threats and any kind of unauthorized use[8]. Cyber security together with the legal framework, is crucial to attract the economic actors and ensure them the cyber environment is safe and protected. Because, each business, institutional, government and private actor is working on a communication device, professionally or privately, and needs security and protection while working. Security should present protection and defense mechanisms against any threat, as well as protect privacy of the individual,

---

[3] Global Cybersecurity Index 2018, ITU Publications, Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[4] Cyberspace. Information Technology laboratory. Computer Security Resource Center. Retrieved from: https://csrc.nist.gov/glossary/term/cyberspace.

[5] "What is Cybercrime". Retrieved from: https://www.bedfordshire.police.uk/information-and-services/crime/cyber-crime-and-online-safety/what-is-cyber-crime#1e3c296b.

[6] S. Das, T. Nayak, *Impact of cyber crime: Issues and challengess*, International Journal of Engineering Sciences & Emerging Technologies, October 2013, Volume 6, Issue 2, pp: 142-153. IJESET. Retrieved from: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

[7] Cybercrime. European Commission. Retrieved from: https://home-affairs.ec.europa.eu/cybercrime_en.

[8] Cyber security definition. IT governance. Retrieved from: https://www.itgovernance.co.uk/what-is-cybersecurity.

the firm or the government and the fundamental human rights. But developing security models and presenting solutions is not always enough, also technical security measures need to be implemented, as well as legal measures to prevent and stop criminals. And these steps should be presented not only nationally but globally[9]. It has to be acknowledged that Cybercrime and cyber-security have expended as international dimensions. And the threats as political conflicts, nuclear wars have lost their spotlight in the international relations arena and in the international politics arena, now the spotlight is given to the nontraditional security issues like cybercrime and cyber security[10].

II. International Legislation

The first ever international treaty to cover the cybercrime topic was the Budapest convention or the Convention of Cybercrime introduced in 2001. The treaty deals with crimes committed on the Internet and computer networks, computer fraud, child pornography, violations of network security and so on. This Treaty was introduced due to the fact that cybercrime has evolved into a threat to human rights, democracy, the rule of law as well as to international peace and stability, and it has a major impact, as well as a threat to social and economic life. To the Convention was added an additional Protocol on Xenophobia and Racism and Additional Protocol which is in preparation. Furthermore, it was created the Cybercrime Convention Committee (TCY) consisting of signatories of the Convention, who's job is to prepare legal instruments, and encourage cooperation among the members. Furthermore, there is another body, the Cybercrime Programme Office of the Council of Europe (CPROC) that helps in assisting the countries to strengthen their capacities in order to conduct proper investigation, prosecution and arbitration of cybercrime[11].

But, despite all of the efforts, International Law is still struggling to address the issue of 'cyber war'. First of all, there is the question whether International law applies whatsoever to cyberspace and in what conditions. The Tallinn Manual process from 2009 gives some instructions, and has acknowledged that the general principles of international law do apply to cyberspace, including "jus ad bellum" (the right to war) and "jus in bello" (the rules and laws governing the conduct of war). Furthermore, the Tallinn manual defines the state responsibility in cyber operations, what actions should be taken during cyber hostilities, and so on but still the rules remain open to interpretation and are open to the evolution of technology and cyber capabilities[12]. Which means that everything is general and can be interpret by different parties differently which presents a big obstacle in the application and functioning of International law.

---

[9] S. Ghernaouti-Hélie, *Measures on cybersecurity*, S. Schjolberg, S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime* 2011, Retrieved from: https://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

[10] N. Kshetri, *Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations*, Electronic Commerce Research 13 (1)/ 2013, pp. 41-69 Retrieved from: https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybercrime_2013.pdf.

[11] Action against cybercrime. Retrieved from: https://www.coe.int/en/web/cybercrime/home.

[12] European Parliament, *Cyber defence in the EU Preparing for cyber warfare?* Briefing 2014. Retrieved from: https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

III. Transitional Countries (Albania and North Macedonia)

III.A. Albania

Albania is a transitional country with a transitional economy. So how does it handle the new challenges that arise from technology and the internet. As we know Albania is trying to become an EU member so not only in cybercrime but in other fields as well it is trying to incorporate EU laws into its own legislation. Its politics, strategies and documents are incorporated to fight the new problems that arise from cyberspace which is in its own sense a new warfare. It has presented documents such as: the Sectorial Strategy of Society of Information; The Document of politics for electronic communication in the Republic of Albania; the Document of politics for development of telecommunication in the Republic of Albania; The decisions of the Council of Ministers for ratification of documents of politics and strategies etc. It also introduced a law on cybercrime and in 2002 has ratified the Convention for cybercrime, while in 2004 it also ratified the additional protocol of this convention. Also, it has introduced provisions as part of the Albanian Penal Code, which are in coherence with the Convention[13]. Furthermore, in 2009, it established the Computer Crime Special Section in the Department against Organized Crime and Serious Crime, Directorate of Financial Crime[14].

Moreover, the Albanian law on cybercrime is divided into two parts. The first part consists of all illegal actions carried out in the sectors of communication technology and computer system. It covers crimes like unauthorized interference, illegal interception, unlawful and unauthorized interference in computer data; illegal and unauthorized access to computer systems. The legislation is intended to protect the integrity of the system, the security, and the privacy of the data contained in the computer systems. The second part includes all the other cybercrime types which are not covered in the first part. So, cybercrime, is considered as the use of technologies to commit crimes in new fashioned ways[15].

Although, Albania has already implemented many laws and strategies it still needs to work hard to develop policies, standards, procedures in order to guarantee cyber security, to offer protection from cyber threats and respect the principles of fundamental rights and democratic freedoms. And all of them must be adjusted to the needs of the country. The best strategy could be: 1. The completion of legal framework in the field; 2. Raising awareness about cyber security; 3. Increasing the knowledge, skills and capacities of expertise on the field of cyber security; 4. The establishment of specialized units; 5. Identification and protection of Critical Information Infrastructure (CIIP); 6. Creation and implementation of basic requirements of cyber security; 7. Increasing investments for growing the security in state networks/systems[16]. Therefore,

---

[13] I. Shtupi, *The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation*, Academic Journal of Interdisciplinary Studies, MCSER Publishing, Rome-Italy, 2015. Retrieved from: https://www.researchgate.net/publication/297897401.

[14] B. Abdurrahmani, *Cybercrime in Albania: A Discourse on Law, Policy and Practice*, European Academic Research Vol. II, Issue 1/ April 2014. Retrieved from: https://www.euacademic.org/ Upload Article/424.pdf.

[15] *Idem.*

[16] A. Shkembi, I. Shtupi, A. Qafa, *The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation*, Academic Journal of Interdisciplinary

if incorporated, these strategies, there will be significant improvement in the field, as well as securing the system and offering stability and prosperity in the cyber sphere.

III.B. North Macedonia

North Macedonia is also a country in transition with a very week transitional economy. But in the cyber sphere it has accomplished a lot of progress. North Macedonia in 2017 had 73.6% homes using internet, as well as 91.2% use by companies. Therefore, it had to develop a National Cyber Security Strategy in accordance with that of the European Union. But there are obstacles in the availability of ICT, especially in relation to the Critical Information Infrastructure (CII) and other Important Information Systems (IIS). Furthermore, the growing use of social media by society and the use of face recognition algorithms, carry a risk for personal data theft and digital identity theft of individuals, theft of legal entities, companies and etc.. Also, the Macedonian society has a low level of awareness of this kind of threats, which can be detected and prevented by different defense mechanisms created by certain cyber security strategies. In order to be successful in applying these strategies there is a need of professionals, educational programs, as well as application of policies[17].

Furthermore the first legislation adopted by North Macedonia was in 2014 and were adopted the Amendments to the Law on Electronic Communications, in 2016 was created the National Computer Incident Response Team MKD-CIRT, in 2018 was adopted the Cyber Security Capacity Assessment, in March 2018 was established the National Cyber Security Working Group and in July the same year was presented the National Cyber Security Strategy for the period of 2018-2022 and at the end of 2018 was adopted the National Cyber Security Action Plan for the period of 2018-2022. The next year were established the National ICT and Cyber Security Council and in 2020 was presented a Draft Law on Security of Network and Information Systems[18]. Therefore there are a lot of bodies, strategies and policies adopted but are they enough or are they implemented properly to protect and safeguard the cyber sphere and all its users.

IV. The European Union

In recent years, in the EU cyber attacks have become a serious concern, due to the threat they can pose to national security, to foreign policy, but also to the economy. Cyberspace, is considered a fifth domain of warfare. Therefore, member states are developing cyber defence and offence capabilities to prepare for any kind of 'cyber war'. Cyber security, has become an important policy issue in many states. The economic costs of preventing cybercrime and cyber espionage are estimated to be between US$300 billion and US$1 trillion, which range from technical concerns to ensuring the

Studies MCSER Publishing, Rome-Italy, 2016. Retrieved from: https://pdfs.semanticscholar. org/cd34/8906b7b5170601c731763dde70a27ed159f4.pdf.

[17] Republic of Macedonia, Republic of Macedonia National Cyber Security Strategy 2018-2022. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/ NS%20Cyber%20Security%202018-2022_ENG.pdf.

[18] ITU Regional Cybersecurity Forum for Europe and CIS.2020. Retrieved from: https://wwwqa.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2020/CSF/S2%20Veljanovska%20-%20Kovachevska.pdf.

security of governments or critical infrastructure and industries, to protection of citizens. The cyber space is a concern not only in the political sphere, but also in the diplomatic, economic and military spheres and at the national and international levels. Cyber attacks have become both a concern for national security and foreign policy. Major cyber incidents have happened in 2007, like the attacks against the Estonian government which led to paralysis of public services for couple of weeks. In 2010, the 'Stuxnet' computer worm, considered one of the most sophisticated cyber weapons to date damaged uranium enrichment centrifuges in Iran nuclear factory[19].

The EU is working hard in regard to this threat and it is much aware of it, opposite of the transitional countries. So far, it has established the Cyber security Act that strengthens the EU Agency for cyber security (ENISA) and establishes a cyber security certification framework. ENISA has a key role in setting up and maintaining the European cyber security certification framework, as well as to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cyber security incidents. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services and will be recognized across the European Union[20].

The Commission and the European External Action Service launched in 2013 the EU Cybersecurity Strategy which outlines the principles that will guide the EU action in this domain among which are the resilience, the reduction of cybercrime, the cyber defense policy and so on[21].

The EU also has adopted a set of legislative proposals on network and information security. The Commission in 2015 has placed cybersecurity at the heart of its political priorities and the fight against it[22]. For the period 2014-2016, the EU has invested €160 million in research and innovation in cybersecurity and it will further invest up to €450 million of H2020 funding for the period 2017-2020[23]. In December 2020, the European Commission and the European External Action Service (EEAS) presented a new EU cybersecurity strategy with aim to strengthen its protection from cyber threats. In March 2021, the Council adopted a cyber security strategy[24].

To conclude, the EU response to the problem is still with many splinters, but there is improvement. The fragmentation can be seen in the operational capabilities but also in the understanding of this domain[25]. Thus, we can see that problems do exist in the EU as well, not only in the transitional countries.

---

[19] European Parliament, *Cyber defence in the EU Preparing for cyber warfare?* Briefing 2014. Retrieved from: https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.

[20] European Commission, *Shaping Europe's digital future.* Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[21] European Commission, *EU cybersecurity initiatives working towards a more secure online environment,* 2017. Retrieved from: https://ec.europa.eu/information_society/newsroom/ image/ document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

[22] *Ibidem.*

[23] *Ibidem.*

[24] Cybersecurity: how the EU tackles cyber threats, European Council. Retrieved from: https://www.consilium.europa.eu/en/policies/cybersecurity/.

[25] N. Van der Meulen, E.A. Jo, S. Soesanto, Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, European Parliament, 2015. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf.

V. China

In 2011 in China, 217 million Chinese became victims of virus attacks, 121 million people had their online accounts hacked, and 8 % were victims to some kind of online scam. Gu Jian of the Chinese Ministry of Public Security confirmed that many government websites experience cyber attacks. Also, in 2009 the Information Office of the State Council, said that over one million IP addresses were controlled and 42,000 websites were hacked[26].

Before its ratification of the Cyber security Law, China had already introduced some laws, rules and regulations passed and implemented covering cyber issues, such as Administrative Measures for Prevention and Treatment of Computer Viruses and Administrative Measures for Hierarchical Protection of Information Security. But it was obvious that they were not enough, so the Cybersecurity Law, indicates that China is focusing on empowering cyber security and protecting its government institutions, businesses as well as its population. The law was adopted by the National People's Congress (NPC) in 2016 after a long year of legislative proceedings and came into effect in 2017[27]. But as it is obvious from the numbers presented above, the cyber domain in China is also very fragile like in most of the countries in the world. And although it does a lot to improve its cyber security and prevent cybercrime with the laws and regulations adopted, it is still fragmented and it needs to improve either by specifying the weak points or investing more in education, experts and tools specifically in this domain. Also, the cooperation on the global level is very important.

In the Global Security Index of 2018 it can be seen that North Macedonia and China have a high national level of commitment in cybersecurity, where as Albania has a medium national level of commitment[28]. So, this commitment should continue on all levels national, international and global.

VI. Conclusion

It can be concluded that the cyber sphere is incorporated in all fields and aspect of life. It is very difficult to bypass its influence and implications on life. We saw that even though countries have implemented different kinds of legislation and even though International law is applicable to this domain still the threat of cybercrime is strong and part of everyday life. The problem should be discussed on all levels of governance and globally since it is a real global problem. With joint forces countries will be able to create a global network or a system that will safeguard and improve the cybersecurity domain.

---

[26] N. Kshetri, *Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations*, Electronic Commerce Research 13 (1)/2013, pp. 41-69. Retrieved from: https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybercrime_2013.pdf.

[27] Overwiew of China's cybersecurity law. KPMG 2017. Retrieved from: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

[28] Global Cybersecurity Index 2018. ITU Publications. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

References

1. Abdurrahmani, B., *Cybercrime in Albania: A Discourse on Law, Policy and Practice*, European Academic Research Vol. II, Issue 1/ April 2014. Retrieved from: https://www.euacademic.org/UploadArticle/424.pdf.
2. Computer Security Resource Center, *Cyberspace. Information Technology Laboratory*. Retrieved from: https://csrc.nist.gov/glossary/term/cyberspace.
3. Das, S., Nayak, T., *Impact of cyber crime: Issues and challengess*, International Journal of Engineering Sciences & Emerging Technologies, October 2013, Volume 6, Issue 2, pp: 142-153. IJESET. Retrieved from: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.
4. European Commission, *Cybercrime*. Retrieved from: https://home-affairs.ec.europa.eu/cybercrime_en.
5. European Commission, *EU cybersecurity initiatives working towards a more secure online environment,* 2017. Retrieved from: https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.
6. European Commission, *Shaping Europe's digital future.* Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
7. European Council, *Cybersecurity: how the EU tackles cyber threats*. Retrieved from: https://www.consilium.europa.eu/en/policies/cybersecurity/.
8. European Parliament, *Cyber defence in the EU Preparing for cyber warfare?* Briefing 2014. Retrieved from: https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.
9. European Parliament, *Cyber defence in the EU Preparing for cyber warfare?* Briefing 2014. Retrieved from: https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.
10. Ghernaouti-Hélie, S., *Measures on cybersecurity*, in S. Schjolberg, S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime* 2011, Retrieved from: https://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.
11. Global Cybersecurity Index 2018, ITU Publications, Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
12. https://www.bedfordshire.police.uk/information-and-services/crime/cyber-crime-and-online-safety/what-is-cyber-crime#1e3c296b.
13. https://www.coe.int/en/web/cybercrime/home.
14. https://www.itgovernance.co.uk/what-is-cybersecurity.
15. https://www.statista.com/statistics/617136/digital-population-worldwide/.
16. ITU Regional Cybersecurity Forum for Europe and CIS.2020. Retrieved from: https://wwwqa.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2020/CSF/ S2%20Veljanovska%20-%20Kovachevska.pdf.
17. Kshetri, N., *Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations*, Electronic Commerce Research 13 (1)/ 2013, pp. 41-69 Retrieved from: https://libres.uncg.edu/ ir/uncg/f/ N_Kshetri_ Cybercrime_ 2013.pdf.
18. Kshetri, N., *Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations*, Electronic Commerce Research 13 (1)/2013, pp. 41-69. Retrieved from: https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybercrime_2013.pdf.

19. Republic of Macedonia, Republic of Macedonia National Cyber Security Strategy 2018-2022. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NS%20Cyber%20Security%202018-2022_ENG.pdf.

20. Shkembi, A., Shtupi, I., Qafa, A., *The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation*, Academic Journal of Interdisciplinary Studies MCSER Publishing, Rome-Italy, 2016. Retrieved from: https://pdfs.semanticscholar.org/cd34/8906b7b5170601c731763dde70a27ed159f4.pdf.

21. Shtupi, I., *The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation*, Academic Journal of Interdisciplinary Studies, MCSER Publishing, Rome-Italy, 2015. Retrieved from: https://www.researchgate.net/publication/297897401.

22. United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Vienna 2013, retrieved from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

23. Van der Meulen, N., Jo, E.A., Soesanto, S., Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, European Parliament, 2015. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf.