Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 143–154

DOI: 10.17951/teka.2018.13.2.143-154

THE UK GOVERNMENT'S RESPONSE TO CYBER THREATS

Jakub Wołyniec

Maria Curie-Skłodowska University. Faculty of Political Science
ORCID ID: https://orcid.org/0000-0001-9411-8568
e-mail: jakub.wolyniec@o2.pl

Abstract: The paper addresses the cyber security issue of the United Kingdom from the perspective of governmental institutions responsible for combating threats coming from cyberspace. The first part of the article presents a catalogue of cyber threats facing various entities in the United Kingdom. In addition, the features of cyberspace that particularly strengthen its vulnerability to these threats are indicated. The second part of the article focuses on presenting institutions and organizations and their actions that are directly or indirectly responsible for cyber security in the UK. First, it focuses on organizations solely responsible for cyber security: from special services (GCHQ), to the National Cyber Security Centre (NCSC), to specialized units operating within these organizations. The article then focuses on other agencies and units operating within government structures, which are related to the Home Office, the Foreign Office and the Ministry of Defence. These include the National Crime Agency, the police, intelligence and counter-intelligence. The paper also presents initiatives of ministries related to social policy, digitization, culture, media, business and enterprises, the protection of which is one of the priorities highlighted in the UK cyber security strategy.

Keywords: cyber security, cyber threats, institutional response, National Cyber Security Programme, United Kingdom

INTRODUCTION

The UK Government has started thinking seriously about its cyber security since the middle of the first decade of this century. The UK's first Cyber Security Strategy, published in 2009, created central cyber security capabilities for the first time. The turning point, however, was the General Election of May 2010 and the subsequent takeover by the Conservative-led coalition government with the Liberal Democrats. The new rule in the UK resulted in the Strategic Defence and Security Review (SDSR) being commissioned and inclusion of cyber-related security issues to the UK strategic thinking in the form of the National Cyber

Security Programme (NCSP). The programme, announced in 2010 with funding in the years 2011–2016, amounting to £860 million, can be described as one national plan of activity, a series of measures, with strategies to support it in other departments [Stoddart 2016: 1087]. Its core aims are "to defend the UK from cyber attacks, deter potential attackers and develop the UK's cyber security industry" [*Cyber Security of UK Infrastructure* 2017]. The National Cyber Security Programme undergoes a yearly review followed by a budget allocation [Bada 2016: 18]. The purpose of this transformative programme revolves around four main elements: "improving national cyber security, improving cyber-defence of critical infrastructure, combating cybercrime and enhancing education and skills" [Downing 2011: 10]. In 2011, the Conservative-Liberal Democrat coalition government released the second cyber security strategy. These documents laid the foundations for the fight against cyber threats. However, they were criticised for being too general in their wording and for having too few suggestions on how to solve the problem related to cyber security [Kozłowski 2014: 56]. In the newest Strategic Defence and Security Review, the government announced that the funds for the continuation of the programme to 2020 will more than double amounting to £1.9 billion [*National Security Strategy and Strategic Defence and Security Review* 2015: 40]. Once a threat is identified in strategic documents, a response must be developed in following policy papers. The National Cyber Security Programme is an example of the UK's attempt to construct coordination between multiple organizations tackling the issue of cyber threats and cyber security.

This paper aims at demonstrating the United Kingdom's national organizational response to growing threats posed by cyberspace, by presenting a catalogue of agencies responsible for security and defence in cyber-related matters in the UK. The first part identifies threats posed by the Internet in a general and UK-specific context. Furthermore, several characteristic features of cyberspace as a virtual entity facilitating cybercrime are described. The second part presents the institutional landscape of organizations involved in a response to the above-mentioned cyber threats. First, the paper introduces organizations that are solely responsible for cyber security such as Government Communications Headquarters and its National Cyber Security Centre. Next, the effort of the British intelligence agencies, such as MI6, MI5 and Defence Intelligence, is presented. Finally, cyber-related initiatives of ministerial departments are described. These include the Ministry of Defence, the Home Office, the Ministry of Housing, Communities and Local Government, the Department for Digital, Culture, Media and Sport, and the Department for Business, Energy and Industrial Strategy. The question arises whether the government of the United Kingdom recognises and fulfils the necessity for a concerted response to cyber threats.

CYBER THREAT LANDSCAPE

A key feature of cyber security is the specific environment in which the need for such security is realised. Cyberspace, unlike physical space, is manmade and is characterised by its virtual nature – it does not exist physically despite consisting of interconnected networks and devices. Although it was created by humans, it has now slipped out of human control. One of the main challenges in connection with cyberspace is lack of governance and control over its current functioning and future expansion, thus, making it an ambiguous and indefinite structure. Another characteristic feature of cyberspace facilitating undesirable and illegal behaviour is that Internet users can feel anonymous to some extent. Cyberspace being an egalitarian, anonymous, non-material creation, devoid of the parameter of geographical space, and constituting a trans-sectoral area of national and international security, is a perfect platform for undesired, harmful activity by state and non-state actors alike.

Before an analysis of the UK cyber security community can be carried out, it is significant to comprehend better the threat landscape with which the UK is confronted. Threats to cyberspace can broadly be divided into two categories. The first category includes threats devoid of human factor, that is, unrelated to human activity. These include, among others, power and communication failures, malfunctioning of hardware or software due to manufacturing defects, natural disasters such as floods, fires, hurricanes, earthquakes, etc. The second category of threats to cyberspace includes threats caused both by intentional and unintentional human activity. Unintentional errors and negligence, such as deficiencies in training people, bypassing procedures and the lack of appropriate knowledge can be and are used to carry out attacks. Intentional attacks motivated by various negative intentions constitute the most dangerous threat to the security of cyberspace. They are for the most part carried out in cyberspace and using cyberspace. The consequences of cyber attacks can be damage or destruction of hardware as well as destruction, seizure or unauthorized access to software and data.

Threats in cyberspace can also be classified in a different manner. In a Chatham House report [Cornish, Hughes, Livingstone 2009: 3–12], revolving around cyberspace and the national security of the UK, the authors proposed a set of four cyber threat domains that demonstrate a vast array of interconnected risks and hazards with which cybersecurity policy-makers must deal. These domains are: state sponsored cyber attacks; ideological and political extremism; serious and organized crime; and lower-level/individual crime. Correlating cyberspace and the UK national security, the authors of the report draw a conclusion that information and communication technologies (ICT) have "an increasingly important enabling function for serious and organized crime, ideological and political extremism, and possibly even state-sponsored aggression" [Cornish, Hughes, Livingstone 2009: 12].

While cyber threats and cybercrime are global phenomena, the UK has not remained unaffected by these problems. According to the National Crime Agency (NCA) report [*Cyber Crime Assessment 2016*], cybercrime has overtaken all other forms of crime in the UK. The report also suggests that the percentage is possibly far worse that the numbers show considering that cybercrime is mostly under-reported by victims. Other sources also confirm that as much as 80% of crime in London is unreported [Stoddart 2016: 1085]. The updates of the situation published in the NCA report one year later provide an insight into sources of the attacks. As stated by the report, although the main threat to the UK from cybercrime stems from Russian-speaking nations, the threat is increasingly global [*National Strategic Assessment of Serious and Organised Crime*, 2017]. On the other hand, there has been voices criticizing the "cyber-organized crime" narrative applied by various government agencies and bodies [Lavorgna, Sergi 2016: 182–183]. The said report reveals that some well-known tendencies hold true: through social engineering, cybercrime still benefits from the exploitation of simple security and human vulnerabilities. Additionally, recent trends have been confirmed as the cybercrime actors are moving towards targeting businesses and their payment systems due to the prospect of higher financial profits [*National Strategic Assessment*..., 2017].

Business on the Isles is increasingly becoming a target of the attacks. In a report outlining various cyber threats to UK business [*The Cyber Threats to UK Business*, 2018], the major incidents impacting entrepreneurs in 2017 included: ransomware and distributed denial of service attacks, massive data breaches, supply chain compromises, fake news and information operations. The above-mentioned are usually possible sources of a profit loss for larger businesses. Nevertheless, small businesses are just as much at risk. Other significant incidents in the UK, according to the report, include: business e-mail compromise fraud, major security vulnerabilities (such as Meltdown and Spectre in January 2018), financial sector compromise, cybercrime as a service (for example, reFUD.me, Cryptex Reborn and Cryptex Lite) and targeting of the Parliament – the case of June 2017 e-mail attack. The proof that ransomware attacks, also mobile, are increasingly widespread is the WannaCry ransomware attack in May 2017. According to the report [*The Cyber Threats to UK Business*, 2018], this rapidly and randomly self-replicating worm infected 300,000 devices in 150 states and affected various services worldwide, including the British National Health Service (NHS). Challenging to the global cyber security community are new threats connected with novel fields within ICT such as the Internet of Things and Big Data [Stoddart 2016: 1080–1081] and new methods used by hostile actors [*Cyber Threats to National Security*].

To tackle various cyber threats, members of the UK cyber security community have to adapt to the changing cyber environment and work closely in partnership to achieve highest possible information assurance. The structure of the community may give hope for achieving the intended objectives, especially in the area

of protecting business and enterprises. It comprises organizations and agencies solely responsible for cyber security and units or teams within other agencies and institutions.

UK'S GOVERNMENT ORGANIZATIONS

The Government Communications Headquarters (GCHQ) located in Cheltenham, with regional hubs in Scarborough, Bude, Harrogate and Manchester, is central to tackling cyber threats in the United Kingdom. It receives approximately half of the NCSP funding [Osula 2015: 11]. The organization is not part of the Foreign and Commonwealth Office, however, it falls within the responsibility of the Secretary of State for Foreign and Commonwealth Affairs. In addition to signals intelligence, the GCHQ also deals with cryptanalysis and cryptography. General aims of the GCHQ are to defend government systems from cyber threats, support the Armed Forces and keep the public safe both online and offline through partnership with law enforcement and other intelligence agencies.

Since 2010, the GCHQ has had a Cyber Security Operations Centre (CSOC) in place, responsible for monitoring the status of computer networks in the UK and coordinating incident response. Although the CSOC focuses on defence, its employees also have offensive capabilities against attackers. Another task of CSOC is to "share with businesses and the public information and advice on attacks against UK networks and users" [Osula 2015: 12]. The Cyber Defence Operations team – formerly known as the Network Defence Intelligence and Security Team – is a part of the GCHQ. By means of increased detection and analysis, the team has significantly improved the UK's protection from cyber attacks [Osula 2015: 11].

In line with global standards, there exists the Computer Emergency Response Team for UK Government (GovCertUK) that works with industry, government, academia and analogous CERT-UK team for individual Internet users created in 2014 to enhance UK cyber resilience [*National Cyber Security Strategy 2016–2021*, 2016: 29]. In addition to responding to incidents, it also coordinates all other CERTs in the UK and raises awareness of cyber threats [Stoddart 2016: 1082].

The Communications-Electronics Security Group (CESG), now renamed the National Technical Authority for Information Assurance as part of National Cyber Security Centre (NCSC), was responsible for encrypted data security and cyber security in government institutions. The institution is responsible for the detection of weaknesses in ICT systems, certification, training and awareness raising of cyber threats. The National Technical Authority for Information Assurance supports the UK Government and is responsible for safeguarding state secrets, maintaining a high level of security in government information and communication systems, securing critical infrastructure and continuity of network access [Osula 2015: 12].

The National Cyber Security Centre (NCSC) is a main cyber security component of the GCHQ. Since 2016, it has been the government's main source of

expertise in cyber issues [*Cyber Security of UK Infrastructure*]. It cooperates with and uses expertise of industry and academia. It also brings expertise from previously established organizations: CESG, the Centre for Cyber Assessment (CCA), CERT-UK and the Centre for Protection of National Infrastructure (CPNI). The NCSC claims that its aim is "to make the UK the safest place to live and do business online" [*About the NCSC*]. NCSC actions have also practical aspect; its flagship event in 2018 – CYBERUK 2018 – was "the largest and most wide ranging event for cyber security leaders and professionals in the UK" [*CYBERUK 2018*]. The NCSC and UK industry came up with a joint initiative and created Cyber Security Information Sharing Partnership (CiSP) to "exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business" [*Cyber Security Information Sharing Partnership*].

In every institution, agency or department dealing with security in general, there is a unit or a team dealing exclusively with cyber security. One of the most important government bodies tasked with supervising all matters related to national security, intelligence coordination, and defence strategy, including cyber security, is a Cabinet Committee named National Security Council established in 2010. It is chaired by the Prime Minister and consists of nine permanent members who are the most senior officials and governmental security-related ministers. One of the four ministerial sub-committees of the Council is responsible for matters relating to cyber programmes and policy development [*National Security Council*].

Within the National Security Secretariat, which provides coordination on security and intelligence issues of strategic importance, there is the Office of Cyber Security & Information Assurance (OSCIA) created by merging the Office of Cyber Security (OSC) with the Cabinet Office's Information Assurance team in 2010. The OSCIA supports ministers and the National Security Council (NSC) in setting priorities for cyber security, guides and coordinates the National Cyber Security Programme and ensures information security. OSCIA's activities also consist of cooperation with partners from the private sector, exchange of information and promotion of best practices as well as support for educational activities and awareness-raising.

It seems that since 2017 the responsibilities of the OSCIA have been transferred to a new body called the Cyber and Government Security Directorate (CGSD). It is also possible the OSCIA was renamed the CGSD since the previous OSCIA's web address redirects to information concerning the CGSD (as of April 2018). According to the information provided on the official government site [*Cyber and Government Security Directorate*], the CGSD's responsibilities include delivering the new National Cyber Security Strategy, managing the National Cyber Security Programme, supporting the establishment of the National Cyber Security Centre (NCSC), continuing to set policy for government security and implementing the findings of the Government Security Review.

Many of the government's cyber security institutions in the UK are subordinate to the Home Office. The office is responsible for matters relating to security, immigration, law and order, and the fight against terrorism. The Home Office is responsible for law enforcement in the United Kingdom and functioning of police Cyber Crime Units, the most important being the Metropolitan Police Cyber Crime Unit (MPCCU) functioning within FALCON (Fraud and Linked Crime Online) unit in London [*Metropolitan Police FALCON Team*]. The City of London Police are responsible for the nationwide fraud and online crime reporting centre – Action Fraud.

In 2013, the then Home Secretary Theresa May supervised the establishment of the non-ministerial government department called the National Crime Agency (NCA) which replaced Serious Organised Crime Agency (SOCA). The NCA deals with serious and organized crime and is committed to fighting cybercrime across the UK. The NCA established partnerships with police, law enforcement, the public sector and private industry. The agency operates across the UK, respecting the devolution of policing in Northern Ireland and Scotland. As stated by the former Director of Intelligence at the NCA, Jamie Saunders, tackling cybercrime "requires a broad-based strategy that recognises the diversity of offences, actors, and motivations" [Saunders 2017: 13]. The strategic response to cybercrime offered by the NCA recognises the need to deploy "the right balance between the 'Four Ps' of the UK Serious and Organised Crime Strategy – PURSUE, PREVENT, PROTECT, PREPARE" [Saunders 2017: 4]. Tasked with keeping children and young people safe from sexual exploitation, abuse and grooming online, within the NCA, is Child Exploitation and Online Protection Command (CEOP) – a law enforcement agency formed in April 2006 as the Child Exploitation and Online Protection Centre and absorbed into the NCA when the agency was established in 2013 [*Child Exploitation and Online Protection Command*].

Within the NCA there is a special unit for cyber security which is able to quickly respond to changing threats – National Cyber Crime Unit (NCCU). Funded from the National Cyber Security Programme, the NCCU works with regional cybercrime police units in order to coordinate joint efforts in response to major cyber threats and supports cyber-security professionals in identifying and understanding the growing use of the cyber environment as a driver of crime. The unit also works with partners within business and industrial sectors, and international law enforcement to provide investigative response in pursuing cybercriminals at a national and international level. In England and Wales, the NCCU works with and helps in training of dedicated cyber security teams (Cyber Crime Units) within all of nine Regional Organised Crime Units (ROCUs). The NCCU's proactive work is aimed at looking for criminal vulnerabilities and preventing criminal opportunities [*National Cyber Crime Unit*].

Apart from the GCHQ, the main cyber intelligence and cyber security organization mentioned above, different aspects of cyber threats are tackled by rest of the United Kingdom intelligence community, especially its main agencies:

the Secret Intelligence Service (MI6), the Security Service (MI5), and Defence Intelligence (DI).

Being an integral part of the Ministry of Defence, Defence Intelligence (DI), formerly known as the Defence Intelligence Staff (DIS), is an organization of the UK intelligence community headed by the Chief of Defence Intelligence (CDI). The Chief's military deputy, Director of Cyber Intelligence and Information Integration (DCI3), is responsible for cyber security and cyber intelligence. Responsible for coordinating cyber security activities and ensuring its coherent integration across the Ministry of Defence was the Defence Cyber Operations Group. Now functioning under the name Joint Forces Cyber Group (JFCyG) it comprises Joint Cyber Units, Joint Cyber Reserve and Information Assurance Units [*Defence Intelligence*].

Civilian special services are also responsible for the fight against cyber threats. Within the Security Service, or MI5, there is a separate branch intended, among others, for cyber security and cyber threats, including cyber espionage and cyber terrorism. Cyber is one of four main areas of operation of MI5 next to terrorism, espionage and proliferation of WMD (weapons of mass destruction). It remains within the UK's vital interests to guarantee risk-free opportunities for business development in the country which is captured by one of MI5 slogans: "Protecting your business and yourself" [*Cyber*, MI5…]. Accountable to MI5 is the Centre for the Protection of National Infrastructure (CPNI) which maintains close relations with industry [Cornish et al. 2011: 18]. The CPNI "advises organizations in the national infrastructure to reduce their vulnerability to terrorism and espionage" using "strong partnerships with private sector organizations across the national infrastructure" it created "a trusted environment where information can be shared for mutual benefit" [*National Cyber Security Strategy 2016–2021*, 2016: 74]. The CPNI is widely considered as being effective and part of "a highly capable network of agencies involved in counterterrorism efforts" [Oleksiewicz 2016: 144]. Since 2016, some cyber-related matters have been transferred to the newly created NCSC. In addition to the MI5 activities, the actions taken by the Secret Intelligence Service (SIS), also known as MI6, are relevant as well; the intelligence provides the government with information on the external cyber threats, and takes action outside the UK to address various threats including cyber terrorism. Similarly to the National Security Strategy, SIS identifies cyber threats as one of the four main areas of security risk to the UK [*Our Mission*].

In addition to the ministries related to security, defence and foreign affairs, other ministries in some part devote their policy to providing cyber security in a broad sense. The Ministry of Housing, Communities and Local Government (MHCLG) publishes guides for local authorities on how to increase regional cyber resilience and avoid and mitigate the effects of cyber attacks on local institutions and small businesses. The British Ministry of Justice is also involved in providing information security by funding the Information Commissioner's Office, which deals with the security of information and data in the context of civil rights pro-

tection. The Department for Digital, Culture, Media and Sport (DCMS), together with business and academia, has developed the Cyber Growth Partnership (CGP) which offers assistance to companies dealing with cyber security solutions in promoting their offer abroad. In addition, through the involvement of universities, the CGP develops research and training programmes on the skills needed to ensure cyber security. DCMS also supports initiatives such as the UK Cyber Security Forum to support innovation in the cyber industry.

The Department for Business, Energy and Industrial Strategy (BEIS) is also a recipient of the National Cyber Security Programme funds [Heitzenrater, Simpson 2016: 44]. One of the most important effects of the NCSP is to increase awareness of the threats and importance of security within the wider business community. BEIS takes action in this area offering funding to companies to invest in improving their cyber security. The department also issued popular among entrepreneurs recommendations containing cyber security guidance for business in a form of ten steps to achieve increased information and communication security. In 2014, the UK Cyber Security Forum was established as a place to share experiences for all companies involved in cyber security. In 2015, the Forum was transformed into a company to expand and intensify its activities.

CONCLUSIONS

The paper has illustrated the vast and comprehensive system of institutional response on the part of the government to the threats posed in cyberspace. Government departments, agencies and organizations support and reinforce one another in order to achieve goals set out in various policy papers. Some partnerships result from the clear indications of the cyber security strategy while others are based on a different premise. As a result of the analysis, four general conclusions can be formulated.

First, one can observe a gradual process of concentration of cyber-related issues transferred from organization dealing with general security (such as the Centre for Protection of National Infrastructure) to specialised organizations such as the National Cyber Security Centre within the GCHQ. Regarding the first national cyber security strategies, some scholars suggested there were too many institutions responsible for cyber security without one coordinating the activities of the others. It had been predicted that it would lead to duplication of competences and functions and might limit the effectiveness of UK cyber security [Kozłowski 2014: 54]. The creation of the NCSC within the GCHQ is an answer to those fears. Nonetheless, it seems to be a little too soon to carry out a comprehensive analysis of the effectiveness of the NCSC and the second stage of the National Cyber Security Programme as they exist only since the late 2016. Paradoxically, as the process of concentration continues, some scholars now estimate that the GCHQ is too powerful in the field of cyber security [Stoddart 2016: 1090].

Second, powerful as they may seem, the GCHQ and the NCSC are subject to the British law and the processes of devolution. In some cases, such as cyber security units in the police, it is difficult to create one national unit with the same powers in England, Wales, Scotland and Northern Ireland. It comes as a challenge for the central and local authorities, as the endangerment of elements of national critical infrastructure in one of four home nations may have grievous consequences to the whole of the UK's security.

Third, the perception of cyber security as part of general security has changed. The new cyber-security strategy assumes increased spending on the second stage of the National Cyber Security Program 2016–2020 of approximately 220% in comparison to the 2011–2016 scheme. The increase from £860 million to £1.9 billion is a sign of how seriously cyber security is viewed by the government. It also shows that cyber security has become a demanding sphere of security.

Finally, contrary to many countries, the UK puts protection of businesses and industry as a priority in the cyber-security strategy. Small and medium-sized enterprises often lack resources and required know-how to protect themselves against cybercrime. Another problem is not sufficient knowledge about possible threats. The government addresses this issue by organising or supporting awareness-raising campaigns and actions through the Department for Business, Energy and Industrial Strategy, the Cyber and Government Security Directorate (CGSD) and Cyber Security Information Sharing Partnership (CiSP).

As the paper has proved, cyber security in the UK's organizations resulting from concepts applied in strategic documents is understood not as a product nor a static condition that can be fully achieved but rather as a process involving trained people, newest technology and implementation of suitable strategies. Given the scale of the challenge, the government of the United Kingdom seems to have recognised the necessity for a concerted response. As continuation is part of UK's political culture, hopefully this thinking will carry on and future national security and cyber security strategies and resulting programmes will be flexible enough to adapt to constantly transforming security environment in order to educate about, identify, protect from, and respond to increasing cyber threats.

Tytuł: Reakcja Wielkiej Brytanii na cyberataki

Streszczenie: W artykule podjęto kwestię cyberbezpieczeństwa Wielkiej Brytanii z perspektywy działań rządowych instytucji odpowiedzialnych za zwalczanie zagrożeń płynących z cyberprzestrzeni. W pierwszej części artykułu przedstawiono katalog zagrożeń płynących z cyberprzestrzeni, z którymi zmagają się różne podmioty w Wielkiej Brytanii. Ponadto wskazano na te cechy cyberprzestrzeni, które szczególnie wzmacniają jej podatność na wspomniane zagrożenia. W drugiej części artykułu scharakteryzowano instytucje i organizacje oraz ich zakres działań bezpośrednich lub pośrednich w kwestii bezpieczeństwa cybernetycznego w Wielkiej Brytanii. Najpierw skupiono się na organizacjach wyłącznie odpowiedzialnych za cyberbezpieczeństwo: począwszy od służb specjalnych (GCHQ), przez Narodowe Centrum Cyberbezpieczeństwa (NCSC), skończywszy na wyspecjalizowanych jednostkach działających w ramach tych organizacji. Następnie

zaprezentowano agencje i jednostki działające w strukturach rządowych związanych z resortem spraw wewnętrznych, spraw zagranicznych i obrony, takich jak Narodowa Agencja ds. Przestępczości, policja, wywiad i kontrwywiad cywilny i wojskowy. Przedstawiono również inicjatywy resortów związanych z polityką społeczną, cyfryzacją, kulturą, mediami oraz biznesem i przedsiębiorstwami, których ochrona jest jednym z priorytetów wspominanych w brytyjskiej strategii cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, zagrożenia cybernetyczne, reakcja instytucjonalna, Narodowy Program Cyberbezpieczeństwa, Wielka Brytania

REFERENCES

1. *About the NCSC*, NCSC, https://www.ncsc.gov.uk/information/about-ncsc [access: 1.04.2018].
2. Bada M. (2016), *Cybersecurity Capacity Review of the United Kingdom*, Global Cyber Security Capacity Centre University of Oxford, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf [access: 2.02.2018].
3. *Child Exploitation and Online Protection Command*, National Crime Agency, https://www.ceop.police.uk/safety-centre/ [access: 30.03.2018].
4. Cornish P., Hughes R., Livingstone D. (2009), *Cyberspace and the National Security of the United Kingdom. Threats and Responses*, Chatham House, London.
5. Cornish P., Livingstone D., Clemente D., Yorke C. (2011), *Cyber Security and the UK's Critical National Infrastructure*, Chatham House, London.
6. *Cyber and Government Security Directorate*, GOV.UK, https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance [access: 18.04.2018].
7. *Cyber Crime Assessment 2016*, National Crime Agency, http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file [access: 30.03.2018].
8. *Cyber Security Information Sharing Partnership*, NCSC, https://www.ncsc.gov.uk/cisp [access: 24.03.2018].
9. *Cyber Security of UK Infrastructure*, (2017), The Parliamentary Office of Science and Technology, http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0554?utm_source=directory&utm_medium=website&utm_term=PN554#fullreport [access: 30.03.2018].
10. *Cyber Threats to National Security*, CPNI, https://www.cpni.gov.uk/cyber [access: 20.04.2018].
11. *Cyber*, MI5 – The Security Service, https://www.mi5.gov.uk/cyber [access: 30.03.2018].
12. *CYBERUK 2018*, NCSC, https://www.ncsc.gov.uk/cyberuks/cyberuk-2018 [access: 30.03.2018].
13. *Defence Intelligence*, GOV.UK, https://www.gov.uk/government/groups/defence-intelligence [access: 24.02.2018].
14. Downing E. (2011), *Cyber Security – a New National Programme*, House of Commons Library, http://researchbriefings.files.parliament.uk/documents/SN05832/SN05832.pdf [access: 30.03.2018].
15. Heitzenrater C.D., Simpson A.C. (2016), *Policy, statistics and questions: Reflections on UK cyber security disclosures*, "Journal of Cybersecurity", vol. 2 (1). DOI: https://doi.org/10.1093/cybsec/tyw008.
16. Kozłowski A. (2014), *Bezpieczeństwo cybernetyczne Wielkiej Brytanii w strategicznych dokumentach Wielkiej Brytanii 2009–2011*, [in:] I. Penier (red.), *Wielka Brytania i Wspólnota u progu XXI wieku. Przeszłość, teraźniejszość, perspektywy*, UŁ, Łódź.

17. Lavorgna A., Sergi A. (2016), *Serious, therefore organised? A critique of the emerging "cyber-organised crime" rhetoric in the United Kingdom*, "International Journal of Cyber Criminology", vol. 10 (2).
18. *Metropolitan Police FALCON Team*, Cyber Security Intelligence, https://www.cybersecurity-intelligence.com/metropolitan-police-falcon-team-2027.html [access: 24.02.2018].
19. *National Cyber Crime Unit*, National Crime Agency, http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit [access: 30.03.2018].
20. *National Cyber Security Strategy 2016–2021*, (2016), HM Government, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [access: 2.02.2018].
21. *National Security Council*, GOV.UK, https://www.gov.uk/government/groups/national-security-council [access: 30.03.2018].
22. *National Security Strategy and Strategic Defence and Security Review 2015*, (2015), HM Government, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf [access: 2.02.2018].
23. *National Strategic Assessment of Serious and Organised Crime*, 2017, National Crime Agency, http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-2017/file [access: 30.03.2018].
24. Oleksiewicz I. (2016), *Dilemmas and challenges for EU anti-cyberterrorism policy: The example of the United Kingdom*, "Teka Komisji Politologii i Stosunków Międzynarodowych", vol. 11 (3).
25. Osula A.-M. (2015), *National Cyber Security Organisation: United Kingdom*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.
26. *Our Mission*, SIS, https://www.sis.gov.uk/our-mission.html [access: 30.03.2018].
27. Saunders J. (2017), *Tackling cybercrime – the UK response*, "Journal of Cyber Policy", vol. 2 (1). DOI: https://doi.org/10.1080/23738871.2017.1293117.
28. Stoddart K. (2016), *UK cyber security and critical national infrastructure protection*, "International Affairs", vol. 92 (5). DOI: https://doi.org/10.1111/1468-2346.12706.
29. *The Cyber Threats to UK Business. 2017–2018 Report*, 2018, National Crime Agency, http://www.nationalcrimeagency.gov.uk/publications/890-the-cyber-threat-to-uk-business-2017-2018/file [access: 30.03.2018].