SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Thoughts on the evolution of national security in cyberspace

Imre Dobák

dobak.imre@uni-nke.hu

https://orcid.org/0000-0002-9632-2914

Institute of National Security, University of Public Service, Hungaria krt. 9-11. Budapest, Hungary

Abstract

Nowadays, the vast majority of the threats to our security come from cyberspace, resulting in a significant transformation of national security systems. Behind these changes, we can find some organisational and capability responses to technological developments, seeing that the function of national security is inseparable from the social environment and its processes. The study examines certain impacts of cyberspace on national security as a system, addressing some features of the changing external environment. The topic is related to the research on the relationship between the information society and security in the 21st century. Therefore, the study explores some processes visible at the international level and reviews some external environment trends in connection with national security. The role of the technological environment and cyberspace has already come to the fore in connection with national security threats. The changes affect the future of national security thinking and the development of principles and methods. It is the task of national security services operating under strict legislation to respond effectively to various threats in a changing environment. All this is only possible through the continuous monitoring of changes in the environment and long-term strategic thinking.

Keywords:

information society, national security, intelligence, cyberspace

Article info
Received: 14 September 2020
Revised: 8 February 2021
Accepted: 8 February 2021
Available online: 8 March 2021
DOI: http://doi.org/10.35467/sdq/133154

Introduction

Regardless of any political and social systems, the existence of a national security sector and organisations can be considered universal in almost all states. Although there are many formulations and interpretations of the concept of "national security" and the issue that it covers, it does not have a generally accepted definition (Akhgar, Yates and Lockley, 2013, p. 4). The concept can be interpreted broadly, often encompassing broader areas of security, and more narrowly, along the lines of the "intelligence services" organisations and tasks. In this interpretation, we can find widespread use of "national security intelligence" in the scientific literature (e.g. Johnson, 2010).

Aside from the examining of the conceptual framework in the present study, it can be seen as a common element that the primary task of national security organisations in every country is to support the decision-makers of the country with accurate, up-to-date information. Their main tasks, according to the given national legislation, are to obtain and analyse information. In the 20th century, specific areas of human and technical information gathering (e.g. SIGINT – Signal Intelligence, HUMINT – Human Intelligence, OSINT Open Source Intelligence, and MASINT – Measurement and Signature Intelligence) developed in the sector for the implementation of these activities. At the same time, in addition to their specific purpose and secrecy, these areas are undergoing constant change, and one of the most important shaping factors is the external technology environment. Accordingly, monitoring the external environment changes plays an important role and they also respond to them by developing their organisations and methods. In this regard, the spread of cyberspace and the information society can be considered as the most significant shaping factor, thus technological issues have become increasingly important in the life of national security services in recent decades.

Looking at the research framework, we can see that cyberspace has been extensively researched in many areas of complex interpreted security, where some factors that previously seemed mystical can be interpreted as special segments. Many elements of this invisible sphere have already received great publicity, the main framework of its operation is provided by some basic legislation open to the public, and the sector has also been examined by scientific research. On the one hand, society's interest can be explained by the ever-changing military and non-military security challenges and threats, particularly the fight against terrorism and, on the other hand, by some issues related to the protection of individuals' privacy.

National security is basically achieved as part of larger security structures, in common with other members of security organisations, which, due to their complex tasks, are involved in many areas of the fight against illegal activities. All of these factors have called for the development of specific intelligence and response capabilities as well as a steady increase in their effectiveness, to which we have seen many international examples in recent years.

This study, which only reflects the author's views, examines the complex relationship between the cyberspace and the national security sector, where national, historical, political factors and the current challenges of the security policy environment, and furthermore the technological and infocommunication environment, have the greatest impact on the structures mentioned above. Hopefully, these ideas can enrich other professional knowledge on the issue.

SECURITY & DEFENCE QUARTERLY

Methods and frame

As a part of the methodological approach, some theories can be formed in the relationship between technological evolution and the sphere of national security, which can be interpreted generally, regardless of the country. All these factors, as well as the examples on the international stage, indicate the direction of future development. The aim of the study is not to provide a complete overview of IT trends, or to fully describe their military and national security aspects, considering that some comprehensive sectoral research and studies (e.g. O'Hanlon, 2018, p. 5) are available on the topic.

Apart from the military aspect, the national security sector in the simplest approach is connected to the ICT world from the direction of its intelligence/information gathering, and its counter-intelligence tasks. In the first case, we can see the transformation of intelligence technologies and methods and the cross-border possibilities of information gathering solutions come to the fore. In this interpretation, the implications of the Snowden case (The Guardian, 2013), mass data collection, metadata, and the collection of information discussed in the EU arena can be highlighted (LIBE Committee Inquiry, 2013). However, in addition to its national security, legal and diplomatic impacts, the scandal also indicated the directions of technological development, e.g. the possibilities of using the growing mass of data for security purposes. (The study does not intend to examine information gathering in more depth, but many methods of gathering information are the same in the course of collecting information for criminal and for national security areas, so we must not forget their different purposes and their specificities. Their separation can be traced in most countries).

The second segment of the issue is the topic of cybersecurity, which includes the protection of state and national systems, the critical infrastructures against cyber attacks, and even the comprehensive issues of system vulnerabilities.

Cyberspace and national security

As a research framework, the study describes some links and trends of cyberspace and the national security sector in the following areas:

- Permanent development of external technology environment;

- Relocating security threats and challenges to cyberspace;

- Creation of new (national) security areas;

- Strengthening the partnership with the civil RDI (Research, Development and Innovation) environment;

- The problem of the lack of qualified expert staff.

Permanent development of external technological environment

In our world, the proliferation of infocommunication solutions, which are already indispensable in our everyday life, is continuous. New technologies and solutions have emerged (e.g. 5G technology, Artificial Intelligence, and the Internet of things) whose consequences for our daily lives are not yet fully known. However, it can be predicted that they will widely transform our everyday lives, but in addition to their positive effects, they may also carry many threats. Think only of the protection of critical infrastructures that use IT solutions, the security of our personal data, or even the problem of distinguishing between real and false information that affects us.

The role of cyberspace is becoming more and more important and the amount of information generated in digital form is growing, which is a good indication of the pace of development. We can see in the relevant literature that the spread of digitalisation, the growing importance of the mobility trend, and the significance of artificial intelligence are all predicted. As was put a decade ago, the "Technology will develop faster than organisations and society can keep up with" (Misuraca and Lusoli, 2010, p. 22). In connection with the further development of the ICT environment, the example of the proliferation of often voiced IoT devices can be highlighted, which can be considered as one of the most vulnerable areas. There are several estimates for IoT devices in the literature (e.g. Global Risk Report, 2020) but, according to an ENISA plausible scenario for Europe in 2025, "80 billion devices (10 per person on the planet) are connected through the internet and the quantities of data produced has been doubling every 2 years" (Di Franco, 2018, p. 8). These indicate a significant increase in the number of devices by billions already, many of which will be targeted by cyber attacks. Thus, the development will also result in extraordinary security exposure, and in response, governments are devoting increasing resources to their cyber defence capabilities.

The development also indicates the importance of technological superiority issues and the "imbalance" in the possession of modern technologies. Dependence on foreign technologies, and thus vulnerability to the equipment, systems and suppliers from other countries, can also indirectly affect the security of a given community (see: Lewis, 2018). The reasons for this can be traced to the fact that the ICT (and the cyberspace related as well) industries have become strategically important. Examples can already be seen on the international stage, think only of the US-China conflict around the economic (and security) importance of 5G technology (see: US Embassy in Luxembourg, 2020). Among the impacts, the dominant role of global ICT actors, often beyond states, cannot be left out. Although it is not discussed in the present study, their expansion reinforces the effects of globalisation and, as an indirect process, the devaluation of geographical and administrative-state boundaries.

Regarding national security, and the ICT environment in recent decades, we have also witnessed such international issues as national security vs. terrorism and complex issues of criminal intelligence gathering, which revealed the problem of social sensitivity related to intelligence gathering (see: Privacy and Civil Liberties Oversight Board, 2014). The fight against terrorism, which intensified in the changed security environment and culminated in 2001, highlighted the issue of the protection of fundamental rights and the limits of collection of information, as well as the cross-border effects of information. With regard to the topic, the debates over encryption vs. national security can also be mentioned, which have received much publicity in the media, e.g. Apple – FBI debate in 2016 (Gery, Lee and Ninas, 2017, p. 2; Budish, Burkert and Gasser, 2018). All these have already happened in the era of global internet, where issues related to the use of ICT tools for illegal and criminal activities have also became apparent.

Regarding national security, the European Parliament's LIBE Committee's investigation into the US National Security Agency's (NSA) secret data collection and mass electronic surveillance of EU citizens between 2013 and 2014 can also be highlighted, as well as the need for data security, regulation and protection of personal data. This also includes the issue of mass metadata processing, which has increased the need for data protection in Europe (see: Regulation (EU) 2016/679).

Relocating security threats and challenges to cyberspace

The extraordinary spread and development of infocommunication technologies undeniably has many positive effects on societies, but we must not forget that these changes have also created new risks and challenges. Due to the diversity of threats from cyberspace, these can affect the activities of a wide range of security agencies. Its various forms can pose threats to the functioning of social-governmental-economic systems and their objectives (e.g. economic crime, espionage against other countries or even against economic actors, terrorism, and disruption of critical infrastructures) can lead to serious security incidents.

Due to the global nature of cyberspace (e.g. a hyperconnected world), the separating role of state borders has changed and threats from distant geographical areas are increasingly being felt (e.g. cyber attack and cyberterrorism). All these issues highlight the importance of international regulatory issues, solutions and collaborations. In addition to geographical factors, the interdependence of certain subsystems of society has also become more complex due to cyberspace. Its reasons can be found primarily in the development of widespread ICT (Information and Communication Technology) solutions over the past 40 years (Nishimura, Kanoshima and Kono, 2019, pp. 22–23).

It is understandable that members of society focus on free access to information, the sense of independence, the mobility, and the wide range of information, but at the same time, we may be confronted with the use of cyberspace for different criminal activities as well (e.g. economic, financial fraud, human trafficking, smuggling, and terrorism). A significant challenge is the use of new (e.g. encrypted) ICT applications and modern tools by criminal groups for their activities, and as a study on cyberspace notes, "Law enforcement still does not have the capability to act as fast as the criminals, who move freely in cyber space and take advantage of the uncertainty of geographical location to keep ahead of law enforcement and of attempts to mitigate their actions." (Di Franco, 2018, p. 9).

While some security threats (cyber attack, malware, ransomware, etc.) require the responses of a specific area of cybersecurity, the other part can be interpreted as a "traditional" security threat (e.g. terrorism) the elements of which (e.g. terrorism-related propaganda, recruitment, and financial support) have gained ground on the World Wide Web. These may already require the use of information gathering and intelligence activities of national security organisations in cyberspace. (The best-known example is the previously mentioned US data collection's activities in the fight against terrorism in the post-millennium period).

Among the threats associated with cyberspace, we must not forget the intensification of those phenomena that are aimed at the external influence of members of society; they can even cause confusion with fake news and false information for their various purposes. In this interpretation, cyberspace can also represent a new space of conflict, where opportunities for deception, influence, and subversion, even from distant geographical areas, can pose threats to national security.

Creation of new (national) security areas

In response to previous trends, we have seen many responses in the field of national security. New ideas and strategies to increase cybersecurity have emerged, organisations have taken shape, and we have witnessed the development of new methods in the post-Snowden era in intelligence interpretation. Numerous studies have been published which also emphasise the role of technical development and capabilities in the field of national security (e.g. Crosston and Valli, 2017; Henricks, 2017), as is exemplified by developments in the areas of national security, CYBINT (Cyber Intelligence), SOCMINT (Social Media Intelligence), or even OSINT on the Internet. The reasons are understandable, as events in cyberspace can directly affect the security of countries, so new methods will necessarily be built into the capabilities of security organisations. Think of the fight against terrorism, organised crime, economic and financial fraud, or simply hybrid warfare, as well as certain elements of information operations.

Services have recognised that they can gain extremely valuable information using cyberspace, so the importance of the internet as a resource for national security organisations has increased.

Capabilities and organisational elements based on technical brackground that ensure the collection of open information (e.g. OSINT) have gradually gained ground in the national security structures of each country. These strive to collect, analyse and evaluate information that is valuable to them with increasingly sophisticated solutions along with specific professionalism. The literature on OSINT related to the Internet can be considered extremely extensive, highlighting that the framework of information gathering, which was previously the privilege of security agencies, has changed, and its open solutions can be made available not only to government agencies but to everyone. Thanks to the free development, opportunities provided by cyberspace, its professional solutions and frameworks have been able to evolve, facilitating the interpretation of widely available open sources.

The social and security impact of global ICT solutions and systems is still significant today. Think only of those events and activities where social sites played an important shaping role (the Arab Spring, mass illegal migration, and terrorism). But we must also reckon with the fact that modern technologies, in addition to helping in everyday life, provide a space for the spread of false information, as well as for influencing and pressuring processes affecting the security of a given nation.

As an example, extremist and terrorist groups effectively use social platforms (social networking sites, video and file sharing, blogs, and chat rooms) to disseminate their ideology, recruite new members, and promote their illegal activities. The SOCMINT was formed as a kind of response, highlighting that the emergence of human activities in real and virtual space is inseparable so that national security work must also adapt to the changing processes of the virtual world. Another significant impact is the mass emergence of digital data and practical examples of its use, i.e. indirectly, the development of data mining technologies (see, for example, the Cambridge Analytica scandal) (Unver, 2018, p. 16), or even the processes of utilising artificial intelligence, which are a subject of social debate.

The area of cybersecurity is the most visible to society, as we are regularly confronted with the phenomenon of cybercrime or cyber espionage and different illegal activities in cyberspace. As Hewling puts it in the first sentence in a study, “the proliferation of cyber-related crimes has become immense and predominant in today’s technologically driven society” (Hewling, 2018, p. 1). The ENISA (Lourenco and Marinos, 2020, p. 5) also draws attention, in its relevant documents, to cyber espionage as a growing threat, affecting not only the states but also their economic sectors or even strategic players important to a given state. According to the ENISA “in 2019, the number of nation-state-sponsored cyberattacks targeting the economy increased and it is likely to continue this way” (Lourenco and Marinos, 2020, p. 2). The document also states that one of the ten cybersecurity challenges is the issue of hybrid threats, where one of the key elements is the spread of disinformation and fake news.

SECURITY & DEFENCE QUARTERLY

Strengthening the partnership with the civil RDI environment

Nowadays, a significant number of the new scientific results are produced by private companies, universities, and various civil research institutes. In different industries, such as in the field of ICT, the time between the emergence of new scientific results and their implementation has been shortened. Thanks to ICT technologies, the research environment has also changed, extremely fast international exchanges of information have become possible, and research connections have been established in virtual space, basically along the needs of the economy. The possibilities of scientific innovation and technological development have changed and new disciplines have emerged (see: Kadtke and Wharton, 2018). All these also require that the national security sectors monitor the emerging new scientific outputs. While during the Cold War, new developments and solutions were mainly transferred from the direction of the military industry to civil society, the reverse is true today. The relevance of the scientific and engineering role of civil society actors, institutions and companies has therefore increased.

The imbalance in technical capabilities and technical development should be mentioned here as well: with regard to cyberspace, it is true that many countries have significant technological advantages in using them for national security purposes. One of the key elements of this is the field of research and development, so those countries that have advanced technologies (e.g. the United States, Great Britain, Germany, France, Israel, China, and Russia) can quickly use the latest scientific results and solutions in their national security systems.

It can also be stated that national security is inseparable from the social environment and its processes, so the relationships between cyberspace, technological issues and national security have become even stronger in recent decades. The solutions that appear here, even for various intelligence (intelligence) purposes, do not differ technologically from the technologies used in the civilian environment. The differences are primarily due to the purposes and the legislative frame for operating.

It is also obvious that the information needs, and even technical application needs in security organisations, can no longer be served without the external infocommunication environment. Different forms of partnership have thus become more and more important. At the same time, the intelligence sector is a specific market for the concerned companies, especially in research and development and in selling their new innovations. This is especially true for countries whose capabilities do not allow them to maintain the necessary development base.

The problem of the lack of qualified expert staff

Nowadays it is no longer possible to ignore the fact that national security organisations must employ people who are familiar with modern technologies. Accordingly, it becomes important to continuously train those who work for the organisations, as well as to recruit new employees who already have these skills. However, the recruitment of younger generations who have already grown up in a digital environment is hampered by several factors. These include the imposition of strict standards and constraints, which are often typical of the national security sector. In response, we can observe the development of new recruitment (Atesş, 2020, p. 190) and integration practices.

Employing new generations is often accompanied by the emergence of new technologies and new professional thinking. It means that the organisations have to be able to

SECURITY & DEFENCE QUARTERLY

adapt quickly to the changing environments and generational characteristics. This poses a double challenge to organisations as, besides changes in the operating environment (e.g. cyberspace), it becomes important for them to employ a skilled, open-minded, young generation. Their employment in the sector is also important because this generation will be the backbone of the national security organisations in the future. These staff will be able to ensure the further development of areas that are also important for intelligence (e.g. CYBERINT, CYBER-HUMINT, and WEB-OSINT) and cybersecurity.

There is currently a lack of well-trained professionals in the field of cybersecurity, to which ENISA also draws attention (Di Franco, 2018). In reference to the frequently cited Cybersecurity Ventures estimate, "the number of unfilled cybersecurity jobs is expected to grow by 350 percent, from one million positions in 2013 to 3.5 million in 2021" (Morgan, 2019). The shortage of labour is also true for organisations responsible for national security, as the labour market can be considered uniform in this respect.

With regard to the issue of the national security sector, we may encounter the same problem, where the acquisition and retention of qualified human resources are hampered by the dynamic opportunities of the market environment for individual careers. In response, we can see the solutions for technical development and the creation of a partnership environment. Such a direction is the scientific and educational partnership with the higher education environment, of which there are widespread examples of national security, especially in the field of cybersecurity. The best-known examples are in the United States (NSA) and in the United Kingdom (the GCHQ). These organisations have widely developed higher education relationships for the development of their cybersecurity areas.

Conclusion – What is predictable?

Most people have mixed feelings about the issue of national security organisations. It is a fact that many elements of their activities could be intrusive, but their application is also accepted in democratic societies, with regard to strict legal frameworks for operating and respect for democratic norms. They fulfil their duties in an extremely dynamic changing environment, where, in addition to the threats and challenges, we can mainly see the effects of the technological environment. All this results in new methods and solutions for maintaining the effectiveness of organisations.

National security is traditionally associated with the collection of information, the issue of lawful interception, as well as the open collection of information that nowadays can be provided with the help of computer solutions, or even the elements of the HUMINT area unfolding in virtual space (CYBER HUMINT). These require the tracing and using of advanced technologies and employing the young generation, who are familiar with the digital world.

Many areas of cybersecurity are also interconnected with national security. These can be considered a priority area, as critical infrastructures, government systems, health care, and even education systems are particularly vulnerable to the functioning of society. Forecasts show that the number of cyber attacks is constantly increasing, causing more and more threats and damage, but at the same time, the defence against them also requires more and more resources.

The RDI activities are expected to become even more important in the future, especially in the field of cybersecurity. The new results and innovations that emerge here can mutually serve the security of both civil society and economic actors and the state, as well as the increased protection of our data and systems.

New research is emerging, e.g. in areas of data science, such as research into anonymised mass data, as the results can contribute to security (such as cybersecurity or even law enforcement, raising the possibility of regional forecasting of security incidents). These include the COVID tracing applications, where the new mobile apps using the anonymised data of citizens could help the fight the spread of the virus. (At the same time, the social and professional debates related to privacy, the created apps should be compliant with data protection and privacy legislation).

Overall, it can be stated that the evolution of the technological environment and the extraordinarily rapid changes in cyberspace directly affect the future of national security, the related thinking, and the development of principles and methods. Looking to the future, technological superiority will play an important role, providing unpredictable benefits to countries with state-of-the-art capabilities and solutions.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Akhgar, B., Yates, S. and Lockley, E. (2013) 'Introduction: Strategy Formation in a Globalized and Networked Age – A Review of the Concept and its Definition', in Akhgar, B., Yates, S. (eds) *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies*. Butterworth-Heinemann. doi: 10.1016/B978-0-12-407191-9.00001-6.

Ateşş, A. (2020) 'Current challenges and trends in intelligence', *Güvenlik Bilimleri Dergisi,* Jandarma ve Sahil Güvenlik Akademisi, pp. 177–204. doi: 10.28956/gbd.736153.

Budish, R., Burkert, H., and Gasser, U. (2018) 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects', *Aegis Series Paper No. 1804*, Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:36291726 (Accessed: 25 August 2020).

Crosston, M. and Valli, F. (2017) An Intelligence Civil War: "HUMINT" vs. "TECHINT", *Cyber, Intelligence, and Security*, 1(1), pp. 67–82.

Di Franco, F. (2018) *Analysis of the European R&D priorities in cybersecurity, Strategic priorities in cybersecurity for a safer Europe*. European Union Agency For Network and Information Security. doi: 10.2824/14357.

Privacy and Civil Liberties Oversight Board (2014) *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*. Available at: https://fas.org/irp/offdocs/pclob-215.pdf (Accessed: 25 August 2020).

Gery, W. R., Lee, S., and Ninas, J. (2017) 'Information Warfare in an Information Age', *Joint Force Quarterly*, 85(2). Available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_22-29_Gery-Lee-Ninas.pdf (Accessed: 25 August 2020).

Global Risk Report (2020) *The Global RisksReport 2020*, Geneva: The World Economic Forum.

Henricks, S. C. (2017) 'Social Media, Publicly Available Information, and the Intelligence Community.' *American Intelligence Journal*, 34(1), pp. 21–31. Available at: www.jstor.org/stable/26497113 (Accessed 14 February 2021).

Hewling, M. (2018) 'Cyber Intelligence: A Framework for the Sharing of Data', Reading: Academic Conferences International Limited. Available at: https://search.proquest.com/docview/2018927092?accountid=6724 (Accessed: 10 September 2020).

Johnson, L. K. (ed.) (2010) *The Oxford Handbook of National Security Intelligence*. Oxford, New York: Oxford University Press. doi: 10.1093/oxfordhb/9780195375886.001.0001.

Kadtke, J. and Wharton, J. (2018) 'Technology and National Security: The United States at a Critical Crossroads', *Defense Horizons*, Institue for National Strategic Studies. Available at: https://inss.ndu.edu/Portals/68/Documents/defensehorizon/DH-84.pdf (Accessed: 10 July 2020).

Lewis, J. A. (2018) 'Telecom and National Security (commentary)' March 13, Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/telecom-and-national-security (Accessed: 21 December 2020).

LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens (2013). Available at: https://www.europarl.europa.eu/committees/en/product-details/20130923CDT71796 (Accessed: 10 August 2020).

Lourenco, M. and Marinos, L. (2020) *ENISA Threat Landscape, from January 2019 to April 2020*, European Union Agency for Cybersecurity. doi: 10.2824/552242.

Misuraca, G. and Lusoli, W. (ed.) (2010) *Envisioning Digital Europe 2030: Scenarios for ICT in Future Governance and Policy Modelling*, EUR 24614 EN, European Commission Joint Research Centre Institute for Prospective Technological Studies, Luxembourg, Publications Office of the European Union. doi: 10.2791/49877.

Morgan, S. (2019) 'Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally by 2021', *Cybercrime Magazine*, 24 October. Available at: https://cybersecurityventures.com/jobs/ (Accessed: 22 December 2020).

Nishimura, H., Kanoshima, E. and Kono, K. (2019) 'Advancement in Science and Technology and Human Societies', in Abe, S., Ozawa, M. and Kawata, Y. (eds) *Science of Societal Safety Living at Times of Risks and Disasters*. Singapore: Springer, pp. 15–26. doi: 10.1007/978-981-13-2775-9_2.

O'Hanlon, M. (2018) *Forecasting change in military technology, 2020-2040*, Washington D.C.: The Brookings Institution. Available at: https://www.worldpittsburgh.org/wp-content/uploads/2019/01/Forecasting-change-in-military-technology-2020-2040-Brookings-2018.pdf (Accessed: 10 August 2020).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 10 August 2020).

The Guardian (2013) 'The NSA Files'. *The Guardian*. Available at: https://www.theguardian.com/us-news/the-nsa-files (Accessed: 10 August 2020).

Unver, H. A. (2018) 'Digital Open Source Intelligence and International Security: A Primer', *EDAM Research Reports, Cyber Governance and Digital Democracy 2018/8*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331638 (Accessed: 15 August 2020).

US Embassy in Luxembourg (2020) *Secretary Pompeo and Secretary Esper Speak at Munich Security Conference 2020*. Available at: https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/ (Accessed: 15 August 2020).