Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats

KRZYSZTOF KACZMAREK

Abstract False, fast-spreading information can mould public sentiment, influence the outcomes of democratic elections, cause tensions in the international arena, and even spark armed conflicts. The degree to which a state is vulnerable to such threats depends largely on the digital competence of that state's general public. Digital competency includes information competencies, which involve the ability to obtain, evaluate and apply information. Deficits in the public's information competencies make the state more vulnerable to be targeted by disinformation – an element of hybrid warfare. This is especially important because there are no technical measures which could be used to counter disinformation online. It seems that the only way to make the state more resilient against cybersecurity threats is by improving the digital competencies, including, in particular, information competencies, of the general public. This, however, requires strong educational outcomes across all educational stages.

Keywords: • digital competencies • information competencies • manipulation • disinformation • cybersecurity • hybrid warfare

CORRESPONDENCE ADDRESS: Krzysztof Kaczmarek, Ph.D., Koszalin University of Technology, Faculty of Humanities, Department of Regional and European Studies, Śniadeckich 2, 75-900 Koszalin, Poland, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

https://doi.org/10.4335/2022.1.3 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Information manipulation is not a new phenomenon. From time immemorial, people have tried to influence and mislead others to achieve their specific ends. The influence patterns used in the past – tied so strongly to human nature and taking advantage of the perceptual weaknesses of humans – continue to be deployed successfully to influence societies and international relations, among others. Initiated by individuals, pressure groups, and entities, deception and misleading are popular means by which to elicit a desirable reaction from the general public. The emergence of new technologies facilitating information flow has greatly expanded the possibilities of influencing members of the public – for instance, through provocations, spreading false information and falsifying data. An enormous leap has been made away from traditional media – press, radio, and television – and towards the Internet, making it possible to send any information, true or false, into the world in a matter of seconds. Cyberspace has become the primary channel for information flow, allowing almost anonymous interferences with information flows (e.g. distorting messages or discrediting certain groups). The Internet can also be used to generate essentially false information, addressed to any target group – locally, regionally and globally – to produce specific effects that are intentional and often harmful to the general public. Moreover, we should not forget about the ever-growing risk of cyberattacks, which are increasingly having impact on public safety. Also of concern is the employment of advanced computer programs to modify source materials (deepfakes), making it easy to discredit public figures, such as politicians and celebrities, or even neighbours.

The more the public is aware about the potential threats, and the more knowledge it has of the cyberspace, the less prone it is to being manipulated. Clearly, one important measure to tackle cyberthreats (such as deepfakes) is to provide younger generations with proper education by devising curricula that teach them to search for and double-check information, as well as to instil the principles of communication. This is where digital competencies of the general public come to the fore – their improvement now seems to be the key objective of security, educational and social policies.

2 Digital competencies vs. information competencies

Technological advancements in access to information have made digital competencies one of the key determinants of the quality of life. Social activity now largely relies on the Internet. Digital artefacts and access to the Internet influence almost all aspects of social and private lives. Yet, cyberspace is not the natural environment of humanity. Consequently, no tradition exists of passing knowledge about the phenomena and processes occurring in cyberspace to future generations. However, in order to analyse how the digital competencies of the general public influence the state's vulnerability to cyberthreats, these competencies need to be defined. It can be assumed that digital competencies include: 1) browsing, searching for, and filtering digital data, information and content; 2) evaluating digital data, information and content; 3) managing digital data, information and content; 4) interacting through digital technologies; 5) sharing through digital technologies; 6) civic engagement through digital technologies; 7) cooperating through digital technologies; 8) netiquette; 9) digital identity management; 10) creating digital content; 11) copyrights and licensing; 12) computer programming; 13) security technologies; 14) personal data and privacy protection; and 15) the ability to solve technical problems.

According to information provided on the Chancellery of the Prime Minister's website (KPRM), digital competencies include: 1) IT competencies – the ability to use devices and software; 2) information competencies – the ability to use online information critically; and 3) functional competencies – the ability to apply the aforementioned competencies in everyday private and professional life (KPRM, 2020).

Contemporary digital devices and the systems that manage them do not require the average user to have extensive knowledge of IT systems and advanced technical skills. Nevertheless, as modern technology continues to evolve, there is a continuing need to stay up-to-date. This particularly concerns the ability to double-check information, especially since fast-spreading false information can cause social unrest and spark armed conflicts. Researchers concerned with this area have stressed that the growing scale of disinformation poses one of the greatest challenges for global security (Aronhime, Cocron, 2021). Also, it is worth emphasising that technology is not the only factor involved in the susceptibility of the general public (or certain sections thereof) to disinformation. Other factors come into play as well, and they are psychological, cultural, economic and political in nature (Tomala, 2021).

A low level of information competency can make the public more susceptible to fake news, whose primary aim is to undermine the authority of the state and trust in its institutions, as well as to shape public opinion by perpetuating a state of apprehension. Fighting disinformation represents a challenge for both public institutions and private businesses. It seems, however, that institutionally implemented legal solutions cannot counter this phenomenon. What is fundamentally important is that there is common awareness among the public that each piece of information found online should be approached critically. This is particularly pertinent to emotionally charged information, such as that involving religion, ethnicity - and vaccination against COVID-19.

According to some researchers, in the context of cybersecurity, the threats posed by information manipulation seem to be more serious than those associated with malware. Indeed, no technical measures exist to protect against such manipulation (Kangasniemi, 2020).

3 Digital competencies of European societies

Digital competencies are becoming increasingly important in today's world. However, there has been little progress in the European Union in recent years as far as improving the basic digital competencies of adult Europeans is concerned. Even though the European Commission has supported Member States and provided them with guidance, there are relatively few EU-funded projects focusing on the basic social skills of adults.

In 2019, a total of more than 75 million working-age adults in Europe did not have at least basic digital skills. This mostly included the elderly, the undereducated and the unemployed. Meanwhile, more than 90% of jobs already require at least basic digital skills.

The European Commission has implemented a number of measures since 2015 to improve the digital skills of European citizens. Between 2016 and 2018, national projects as part of the "Digital Skills and Jobs Coalition" provided almost 11 million Europeans with the opportunity to improve their digital skills. Almost half of them were primary and secondary school students. However, no data exists as to how these measures ultimately influenced the objectives of this initiative.

Efforts in specific areas of basic digital skills for adults are often part of broader initiatives. This makes it impossible to determine the total amount of EU funds spent exclusively for this purpose. Nevertheless, existing data suggest that the resources available specifically for efforts to improve digital skills among adults are relatively scarce – for instance, projects that specifically involved teaching digital skills in Member States represented only about 2% of the European Social Fund's overall budget for 2014-2020, even though they enjoy a priority status.

Table 1: The percentage of European residents with at least basic digital skills in 2019

Country	Percentage of individuals who have basic or above basic overall digital skills
European Union – 27 countries (from 2020)	56
Belgium	61
Bulgaria	29
Czechia	62
Denmark	70

Germany	70
Estonia	62
Ireland	53
Greece	51
Spain	57
France	57
Croatia	53
Italy	42
Cyprus	45
Latvia	43
Lithuania	56
Luxembourg	65
Hungary	49
Malta	56
Netherlands	79
Austria	66
Poland	44
Portugal	52
Romania	31
Slovenia	55
Slovakia	54
Finland	76
Sweden	72
Iceland	85
Norway	83
Switzerland	77
United Kingdom	74

North Macedonia	32
Albania	21
Serbia	46
Turkey	36
Bosnia and Herzegovina	24
Kosovo	28

Source: (Eurostat, 2021).

In all these countries, the biggest deficits in digital skills were associated with searching for and verifying information online, as well as familiarity with the basic safety rules and measures (Techrush, 2021). The deficits varied, however, between states.

Despite the Member State's investments made in recent years to develop digital infrastructure for educational and training purposes, significant differences continue to exist both between and within the Member States. Contrary to popular belief that young people are the digital generation, study results have shown that a large part of this population have underdeveloped digital skills. Indeed, in all the studied countries, more than 15% of all students did not have adequate digital skills (European Commission, 2020). Moreover, according to OECD data, secondary school teachers in Europe rarely receive training in the use of ICT for educational purposes, and teachers themselves have voiced their need to develop professionally in terms of ICT skills (Europa Nu, 2021). These data suggest that there is no significant correlation between the age group and digital competence. Each group includes people with different levels of knowledge and skills.

4 Threats associated with deficient digital competencies of the general public, with special focus on information competencies

Cyberspace threats to the functioning of societies and states stem not from the existence of ICT infrastructure *per se*, but from the possibilities it affords. In the literature on this subject, the seven most-mentioned sources of cyberattacks include: 1) states – cybernetic attacks launched by a state against another state can disrupt communications, operations of state services and everyday lives of citizens. Here, an attack may be part of hybrid warfare; 2) criminal groups – these aim to infiltrate systems or networks for financial benefits. They deploy phishing, spamming, spyware and malware techniques to steal identity, commit online fraud and engage in extortion; 3) hackers – they explore various cybernetic techniques to break through security defences and to take advantage of security gaps in computer systems and networks. They are motivated by private gain, retribution, persecution, financial benefits or political activism. Hackers devise new types of threats to enjoy recognition in their community; 4) terrorist groups – terrorists mount cyberattacks to destroy, infiltrate, or take advantage of critical infrastructure to pose a threat to national security, take control over military equipment, disrupt the economy and cause mass casualties; 5) hacktivists – they launch cyberattacks for political reasons, not for financial benefit. They target industries, organisations, or individuals that disagree with their political ideas; 6) "malicious insiders" – these may include employees, external suppliers, contractors, or other business partners that have legal access to business assets and use it for fraudulent purposes to steal or destroy information for financial or personal gain. Malicious insiders usually target businesses, but they also attack state institutions; 7) corporate espionage – corporate spies engage in industrial or business espionage to either gain profit or disrupt the operations of a competitive business by attacking critical infrastructures, stealing company secrets, and gaining unauthorised access. Attacks coming from these individuals may also compromise state security when targeting critical sectors of the economy (StealthLabs, 2020).

Each of these cyberattack sources may employ techniques devised to influence social behaviour and sentiment. With the combination of big data and communication automation through bots and artificial intelligence, it is now possible to distribute information that is both personalised and intended for mass audiences. Data and information theft or extortion, takeover of control over websites and news portals, identity theft, deep fakes – all these can be used to mislead the public, and in extreme cases, to cause social unrest and even armed conflicts. The only effective way to tackle these phenomena is by raising public awareness about their existence.

Reasonable decision-making depends on the individual's ability to analyse available information and to make decisions based on it. In extreme cases, decisions made on the basis of false or incomplete data might cause threats not only for the individual making the decision, but also for the general public and the state.

Researchers from the Max Planck Society have identified four primary challenges facing those responsible for tackling manipulation in the public: 1) user behaviour is often influenced by manipulative website architectures, so-called dark patterns (often leading to undesirable behaviour) – advertisements that appear as website content or navigation guides designed such that a click redirects the user to a website extorting data. These may also include misleading privacy settings, causing the user to provide access to more information than they agreed; 2) AI-operated information architectures do not present information neutrally, but in a personalised manner based on data they gather. This means that two people who enter the same search query in a search engine will probably obtain different results. Such outcome could be helpful when the user is looking for a product or service close to their current location. However, the display of news and political contents based on user preferences can lead to information bubbles, where it is impossible to become familiar with alternative opinions; 3) false and misleading information. Videos and posts with conspiracy theories and unsubstantiated rumours can quickly spread through social media and cause harm – for instance, by discouraging people from vaccinating through disinformation about vaccines, putting them and other around them at risk of infection; 4) distracting online environments are constantly trying to draw the attention of users. This equally involves push notifications, displays, pop-up advertisements and streams of ever-changing content. The goal is to draw attention from users and make sure to keep them engaged as long as possible. It is a business model and services utilise it, and it is often the case that users spend much more time online than planned without any actual benefits and at the cost of losing time. At the same time, researchers stress that there are no tools to ensure that online manipulations and spread of disinformation are prevented. However, they claim that a combination of intelligent cognitive tools and education in information use with the adoption of anti-manipulation policies by online platforms could significantly reduce the impact of false information on public opinion and human behaviour (Max-Planck-Gesellschaft, 2021).

5 Conclusion

With the widespread access of the Internet and the digitisation of social activities, cyberspace has become the arena for conflicts between states and blocs of states, as well as intelligence wars. One aspect of such conflicts is the so-called information warfare. The deeper the digital skills deficit of the targeted state, the more effective such warfare is. This includes both the public's susceptibility to various types of disinformation and its ability to follow safety rules.

While cyberspace threats cannot be eliminated, it seems that the only non-technical way to reduce vulnerability to them is to educate and raise popular awareness of them. This applies to the general public and all types of cyberspace activities – private, social, professional and political. However, in order for such education to deliver the expected outcomes, it is necessary to improve the digital competencies of the people in charge of it. The reason this is so important is that with the widespread access to the Internet and with rapid technological advancements, existing threats might evolve, or new, unknown ones might emerge. It is likely that in the near future, we will not be able to tell if we are talking to a machine or a human when using instant messaging applications – and this includes not only voice, but also video communication.

The ability to search for and double-check information should be one of the educational outcomes across all educational stages. The public can become more resilient against information warfare once it has a more critical approach to, and can distance itself from, information (especially that which arouses emotions), thus effectively making the state less vulnerable to cyberthreats.

References:

Aronhime, L. & Cocron, A. (2021) *Przeciwdziałanie dezinformacji – wzmocnienie cyfrowej Odporności Sojuszu,* available at: https://www.nato.int/docu/review/pl/articles/2021/08/12/przeciwdzialanie-dezinformacji-wzmocnienie-cyfrowej-odpornosci-sojuszu/index.html (April 20, 2022).

Europa Nu (2021) *Onderwijs en opleiding: basisvaardigheden en digitale vaardigheden essentieel voor onderwijs, werk en leven,* available at: https://www.europa-nu.nl/id/vldphhf4ak7y/nieuws/onderwijs_en_opleiding_basisvaardigheden?ctx=vj5cj4qyvkgm &tab=0 (April 20, 2022).

European Commission (2020) *Education and Training Monitor 2020,* available at: https://op.europa.eu/webpub/eac/education-and-training-monitor-2020/countries/countries.html (April 20, 2022).

Eurostat (2021) *Individuals' level of digital skills,* available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i/default/table?lang=enidw (April 20, 2022).

(2021) *Mensch versus Internet: Was können wir tun, um uns vor Manipulation, Fake News und Co. zu schützen?*, available at: https://nachrichten.idw-online.de/2021/02/12/mensch-versus-internet-was-koennen-wir-tun-um-uns-vor-manipulation-fake-news-und-co-zu-schuetzen/ (April 20, 2022).

Kangasniemi, H. (2020) *Sosiaalisen manipuloinnin avulla yritetään saada ihminen huomaamattaan luovuttamaan arvokkaita tietoja tai rahaa. Kyberrikolliset ovat ottaneet keinon tehokäyttöön ja se koskee meitä kaikkia,* available at: https://elisa.fi/ideat/tunnista-ja-torju-sosiaalinen-manipulointi/ (April 20, 2022).

KPRM (2020) *Kompetencje cyfrowe,* available at: https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe (April 20, 2022).

Max-Planck-Gesellschaft (2021) *Selbsthilfe gegen Manipulation im Internet,* available at: https://www.mpg.de/16406549/0211-bild-mensch-versus-internet-was-koennen-wir-tun-um-uns-vor-manipulation-fake-news-und-co-149835-x (April 20, 2022).

Spiegel (2021) *EU muss mehr digitale Kompetenzen fördern,* available at: https://www.bildungsspiegel.de/news/weiterbildung-bildungspolitik/4749-eu-muss-mehr-digitale-kompetenzen-foerdern (April 20, 2022).

StealthLabs (2020) *Cyber Security Threats and Attacks: All You Need to Know,* available at: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/ (April 20, 2022).

Techrush (2021) *Analyse in Europa: Vielen Erwachsenen fehlt es an Digital-Kompetenz,* available at: https://techrush.de/analyse-in-europa-vielen-erwachsenen-fehlt-es-an-digital-kompetenz/?cookie-state-change=1631368316921 (April 20, 2022).

Tomala, L. (2021) *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie,* available at: https://naukawpolsce.pap.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak (April 20, 2022).