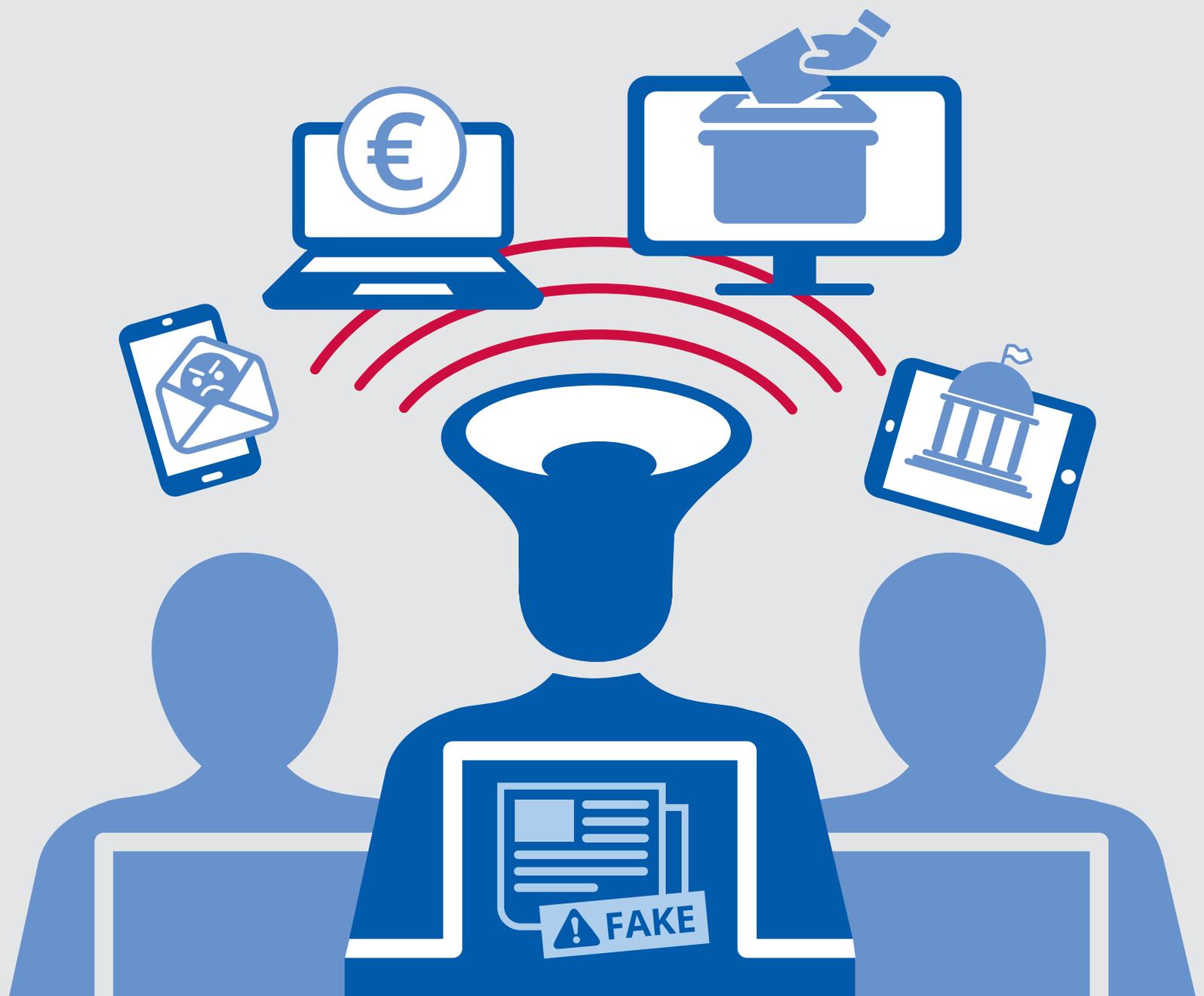


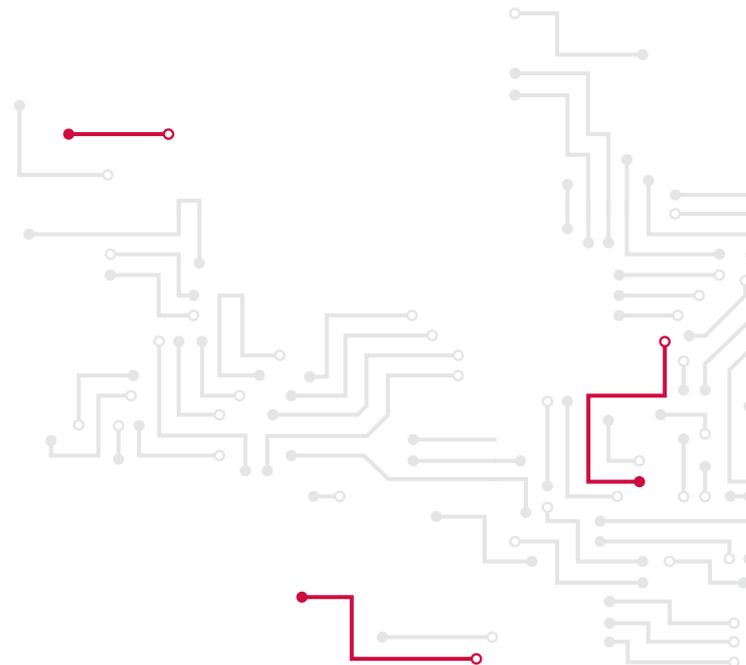
# STRENGTHENING NETWORK & INFORMATION SECURITY & PROTECTING AGAINST ONLINE DISINFORMATION ("FAKE NEWS")

April 2018



# TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>3</b>
<b>2. CONSIDERATIONS SPECIFIC TO ONLINE DISINFORMATION</b>	<b>4</b>
2.1 Artificial Intelligence and Online Disinformation	4
2.2 Economic Disincentives	4
<b>3. CONSIDERATIONS ON GENERAL NETWORK AND INFORMATION SECURITY</b>	<b>5</b>
3.1 Password management	5
3.2 Election systems and infrastructure to be classified as critical infrastructure	5
3.3 Privacy and Data Protection	6
<b>4. RECOMMENDATIONS</b>	<b>7</b>
4.1 Recommendations Specific to Online Disinformation	7
A Artificial Intelligence	7
B Reputation Reporting and Transparency	7
C Economic Disincentives	7
D Source Verification	7
E Online Reporting Options	7
4.2 General Network and Information Security Recommendations	7
F Mandatory Minimum Security Requirements for Passwords	7
G Election Systems, Processes and Infrastructures to be Classified as Critical Infrastructure	7
H Network and Information Security Obligation for Political Organizations	7
I Compliance with Data Protection Requirements	7



# 1. INTRODUCTION

"Fake news"<sup>7</sup> has recently received a lot of media attention as a potential disruptor of democratic processes globally. There is a need to initiate a dialogue in the EU around the possible responses to this phenomenon.<sup>8</sup>

In this regard, the misuse of:

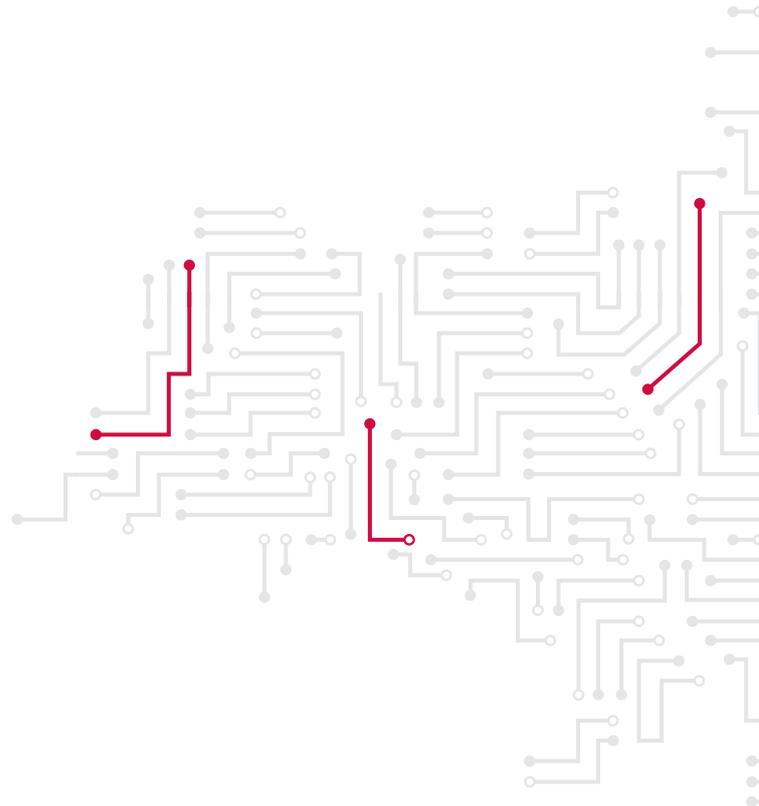
- a computer connected to the internet,
- a compromised online account,
- a fake online account, or
- online platforms

may be characterised as a weapon, where posting on social media, emails, spam and other online activities can cause damage to others, as well as to society at large.

Recent events suggest that the dissemination of online disinformation is posing an increasing threat to the effective functioning of the democratic process. This trend is exemplified by the 2016 U.S. presidential elections where, in a December 2016 survey, 64% of U.S. respondents held that fake news caused a great deal of confusion about the basic facts of contemporary events.<sup>9</sup> Subsequent allegations of cyber meddling in elections in the EU context reported in the media include the French presidential elections<sup>10</sup> and the British EU membership referendum<sup>11</sup>.

A key factor in the dissemination of online disinformation is human behaviour. According to research findings, false claims are shared more than true ones, and false stories gain more attention and are disseminated at a higher speed.<sup>12</sup> Equally important is the amplifier phenomenon, which concerns accounts that disseminate large amounts of false information aimed at manipulating public opinion.

In this paper, ENISA presents some views on the problem of online disinformation in the EU from a Network and Information Security (NIS) perspective. A number of recommendations are presented which relate both to general NIS measures, as well as targeted measures to protect against online disinformation specifically.



7 For the purpose of this paper, "online disinformation" is defined as: "false, inaccurate, or misleading online information designed, presented and promoted with malicious intent or for profit".

8 European Commission (2018). "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation". <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

9 Barthel, M., Mitchell, A., & Holcomb, J. (2016). "Many Americans believe fake news is sowing confusion". Pew Research Center, 15, p. 12. <http://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/>.

10 See: ENISA (2017). "Disinformation operations in cyber-space". <https://www.enisa.europa.eu/publications/info-notes/disinformation-operations-in-cyber-space>.

11 See: Deutsche Welle (2018). "What role did Cambridge Analytica play in the Brexit vote?", available at: <http://www.dw.com/en/what-role-did-cambridge-analytica-play-in-the-brexit-vote/a-43151460>; Scott, M. (2018). "Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower". Politico, available at: <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/>

12 See: Lohr, S. (2018). "It's True: False News Spreads Faster and Wider. And Humans Are to Blame". The New York Times. <https://www.nytimes.com/2018/03/08/technology/twitter-fake-news-research.html>, see also: Vosoughi, S., Roy, D., and Aral, S. (2018). "The spread of true and false news online". Science, 359(6380), 1146-1151. <http://science.sciencemag.org/content/359/6380/1146>.

## 2. CONSIDERATIONS SPECIFIC TO ONLINE DISINFORMATION

### 2.1 ARTIFICIAL INTELLIGENCE AND ONLINE DISINFORMATION

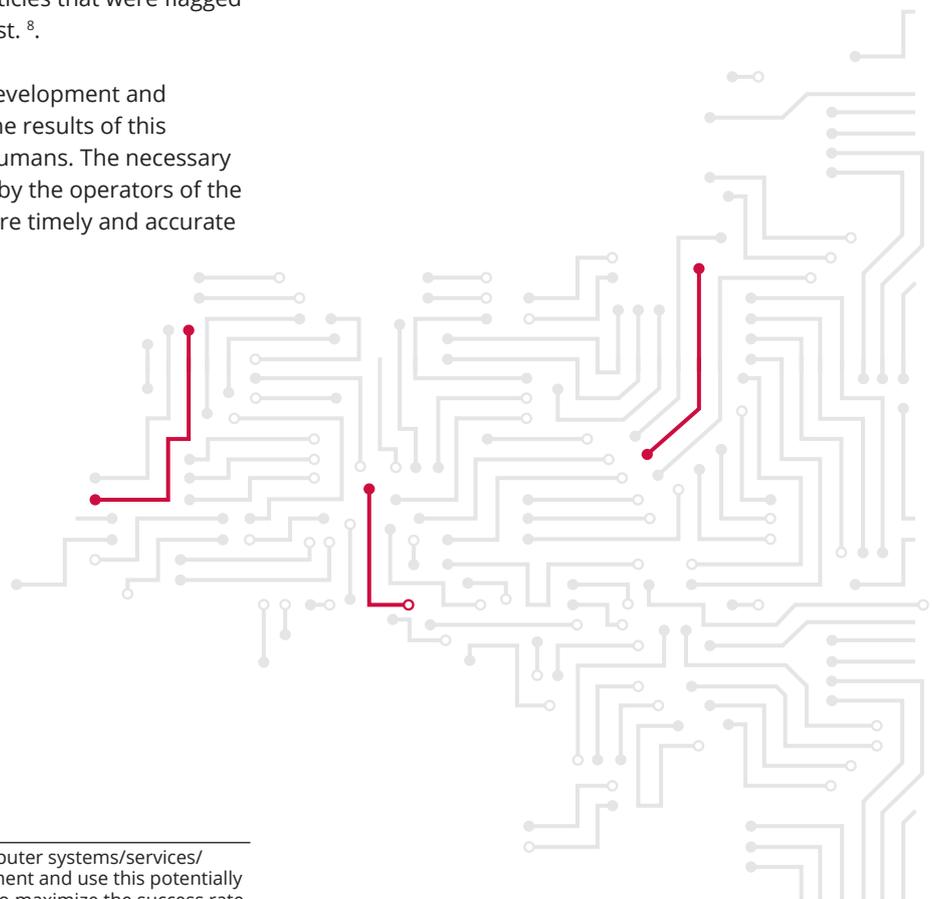
Artificial Intelligence (AI)<sup>7</sup> techniques and methods can range from simple decision making algorithms, to pattern recognition and data mining, as well as to deep learning and other reinforcement learning techniques to name a few.

In the digital era, where information is spreading around the globe in a few seconds, manual fact checking is not an effective and efficient way to address the problem of online disinformation. AI is being leveraged to find words or even patterns of words that can throw light on fake news stories. AI is now looked upon as the cornerstone to separate the good from the bad in the online news field. That is because AI makes it easy to learn behaviours, possible through pattern recognition. Harnessing AI's power, online disinformation can be identified by taking a cue from articles that were flagged as inaccurate by people in the past.<sup>8</sup>

As this technology is still under development and there is a risk of false positives, the results of this analysis should be validated by humans. The necessary resources should be put in place by the operators of the relevant online platforms to ensure timely and accurate management of this issue.

### 2.2 ECONOMIC DISINCENTIVES

Consideration should be given also to the economic drivers used alongside the dissemination of online disinformation. A strategy that could create economic disincentives could include the cutting off of advertising for sites that are found to be involved in the dissemination of online disinformation<sup>9</sup>.



<sup>7</sup> AI in computer science refers to computer systems/services/applications that perceive their environment and use this potentially incomplete data from the environment to maximize the success rate of completing a certain task.

<sup>8</sup> A recent study presents the new developments in this area: <https://www.technologyreview.com/s/609717/can-ai-win-the-war-against-fake-news/>.

<sup>9</sup> Caplan, R., Hanson, L., and Donovan, J. (2018). "Dead Reckoning: Navigating Content Moderation After "Fake News"". Data & Society. [https://datasociety.net/pubs/oh/DataAndSociety\\_Dead\\_Reckoning\\_2018.pdf](https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf).

# 3. CONSIDERATIONS ON GENERAL NETWORK AND INFORMATION SECURITY

## 3.1 PASSWORD MANAGEMENT

As mentioned above, compromised online accounts can be considered as a weapon that can do damage. To preserve the integrity of the account and prevent the impersonation of the user, strong password management is a necessity. Recognising the frailty of human behaviour and the actions currently needed by the user to protect their passwords, the operators of online platforms should take a more proactive role in this process.

It is therefore recommended that for access to all online platforms:

- Algorithms should be deployed that mandate users to have strong passwords in place (long passwords including special characters).
- The use of two-factor authentication should be mandated. The use of two-factor authentication can provide an additional independent level of verification.
- It should be mandatory to change passwords periodically, e.g. every three months.

This approach should help to significantly reduce the number of compromised online accounts that can do damage.

## 3.2 ELECTION SYSTEMS AND INFRASTRUCTURE TO BE CLASSIFIED AS CRITICAL INFRASTRUCTURE<sup>10</sup>

Recently, it has been claimed that political elections in the EU have been undermined by the dissemination of online disinformation. This threat potentially interferes with the democratic process in the EU. Appropriate solutions are needed without unduly limiting the freedom of expression or the fundamental values enshrined in the Lisbon Treaty.

<sup>10</sup> Critical infrastructure can be defined as “an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens”. See: [https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en).

ENISA proposes that legal obligations should be introduced at an EU level to ensure a harmonised approach across all Member States, thereby safeguarding the democratic process across the Union:

- To strengthen the resilience and robustness of the elections systems, processes and infrastructures by classifying them as critical infrastructure. The effect of this classification would be to place an obligation on the responsible stakeholders to implement a high level of network and information security. An option is to use the model of the existing NIS Directive<sup>11</sup>, and classify ‘Election systems, processes

A callout box with a red border and a white background, containing a red text block. A line connects the top-left corner of the box to the text above it.

**Recognising the frailty of human behaviour and the actions currently needed by the user to protect their passwords, the operators of online platforms should take a more proactive role in this process**

and infrastructures’ as a critical infrastructure. This approach would in effect place an obligation on the appropriate stakeholders to take the appropriate and necessary measures to safeguard their network and information security. Furthermore, this approach would also give the stakeholders access to the computer security incident response teams (CSIRTs), which have been built up in all member states pursuant to the requirements of the NIS Directive.

- To explore creating a legal obligation for political

<sup>11</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, available at: <http://data.europa.eu/eli/dir/2016/1148/oj>.

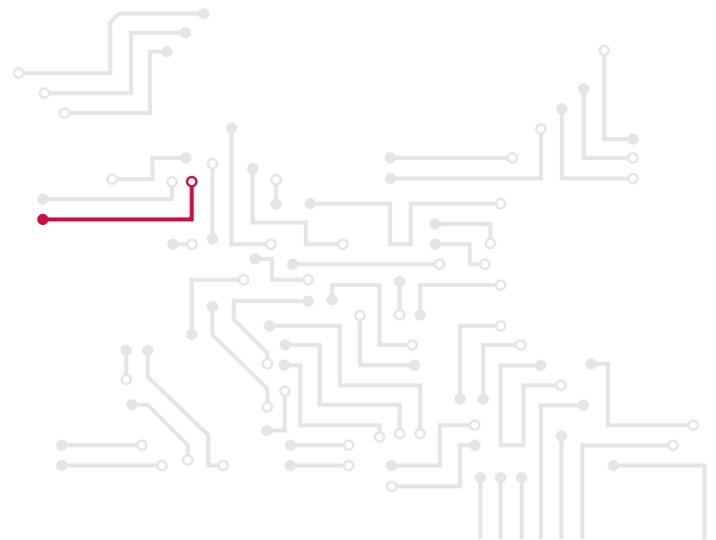
organizations, represented in the National, Regional and European Parliaments, to deploy a high level of network and information security in their systems, processes and infrastructures. In order to support the delivery of this objective, it is suggested that national Competent Authorities<sup>12</sup> in network and information security could assist these organizations on request<sup>13</sup>.

Lastly, the EU is not alone in targeting this rising threat. As several Member States have already taken action to identify and mitigate the risks associated with online disinformation in cyberspace best practices should be shared.

Solutions and research being carried out by third countries should also be considered in the EU context.

### 3.3 PRIVACY AND DATA PROTECTION

Had the General Data Protection Regulation (GDPR)<sup>14</sup> been in effect, strict adherence to it could have prevented the personal data processing patterns that were recently revealed in the media<sup>15</sup>. Given the impending introduction of the GDPR with its extraterritorial effect, this legislation should go a long way to improving protection of personal data. Reasonable security measures<sup>16</sup> and privacy enhancing technologies (PETs)<sup>17</sup> such as use of data minimisation, anonymization, encryption<sup>18</sup>, and attribute-based credentials should be deployed by operators of online platforms.



<sup>12</sup> As defined in the NIS Directive, Supra note 8, Article 8.

<sup>13</sup> For example: in DE, NL, and FR, arrangements along these lines have already been implemented.

<sup>14</sup> 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), OJ L 119, 4.5.2016, p. 1–88, available at: <http://data.europa.eu/eli/reg/2016/679/oj>.

<sup>15</sup> Nicholls, S. (2018). “Could new EU data protection law have stopped the Cambridge Analytica scandal?”, Euronews. <http://www.euronews.com/2018/04/11/could-eu-s-new-data-protection-law-have-stopped-cambridge-analytica-scandal->.

<sup>16</sup> ENISA (2013). “Recommended cryptographic measures - Securing personal data”, available at: <https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data>.

<sup>17</sup> ENISA. “Privacy by Design”, available at: <https://www.enisa.europa.eu/topics/data-protection/privacy-by-design>.

<sup>18</sup> ENISA (2016). “Opinion Paper on Encryption, Strong Encryption Safeguards our Digital Identity”, available at: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption>.

# 4. RECOMMENDATIONS

## 4.1 RECOMMENDATIONS SPECIFIC TO ONLINE DISINFORMATION

### A. ARTIFICIAL INTELLIGENCE

The use of AI algorithms should be deployed to assist in the detection of online disinformation campaigns and misuse of online platforms such as scraping, spam, etc. The outputs of these algorithms should be verified by humans before any action is taken.

### B. REPUTATION REPORTING AND TRANSPARENCY

Online platforms should consider deploying the results from their disinformation analysis and reporting in a transparent manner to build a confidence score on the content, which is presented to the end-user. This approach should build confidence for end-users in analysing the content presented.

### C. ECONOMIC DISINCENTIVES

A strategy should be developed to create economic disincentives, which could include the cutting off of advertising for sites that are found to be involved in the dissemination of online disinformation.

### D. SOURCE VERIFICATION

Online media operators should develop signatures that could be included in their news articles, where users can verify the source of the content.

### E. ONLINE REPORTING OPTIONS

Online platforms should clearly identify reporting locations for the ordinary user to report suspected online disinformation. The reports should be examined in a timely manner by the operators to decide on the appropriate action. The operator should have the necessary resources in place to address the challenge arising from this activity.

## 4.2 NETWORK AND INFORMATION SECURITY RECOMMENDATIONS

### F. MANDATORY MINIMUM SECURITY REQUIREMENTS FOR PASSWORDS

It is recommended that for access to all online platforms:

- i. Algorithms should be deployed that mandate users to have strong passwords in place.
- ii. The use of two-factor authentication should be mandated.
- iii. It should be mandatory to change passwords periodically, e.g. every three months.

### G. ELECTION SYSTEMS, PROCESSES AND INFRASTRUCTURES TO BE CLASSIFIED AS CRITICAL INFRASTRUCTURE

A legal obligation should be considered to classify election systems, processes and infrastructures as critical infrastructure to ensure that they are operated with a high level of network and information security.

### H. NETWORK AND INFORMATION SECURITY OBLIGATION FOR POLITICAL ORGANIZATIONS

A legal obligation should be considered that political organizations are required to deploy a high level of network and information security in their systems, processes and infrastructures.

### I. COMPLIANCE WITH DATA PROTECTION REQUIREMENTS

Reasonable security measures and privacy enhancing technologies (PETs) such as use of data minimisation, anonymization, encryption, and attribute-based credentials should be deployed by operators of online platforms.

# ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu).

## CONTACT

For media enquires about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).

## LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

## COPYRIGHT NOTICE

© European Union Agency for Network and Information Security (ENISA), 2018

Reproduction is authorised provided the source is acknowledged.

