THE EU CYBERSECURITY AGENCY

AFTER ACTION REPORT

MAY 2019

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 Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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.

CONTACT

For contacting the authors please use Excon.EUELEx2019@cooperation.enisa.europa.eu.

For media enquiries about this paper, please use 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

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

On April 5th, the European Parliament, the European Commission and the EU Agency for cybersecurity (ENISA) in close cooperation with the EU Member States organised an exercise to test the EU's response to and crisis plans for potential cybersecurity incidents affecting the EU elections.

The objective of the exercise, which took place in the European Parliament, was to test how effective EU Member States and the EU's response practices and crisis plans are and to identify ways to prevent, detect and mitigate cybersecurity incidents that may affect the upcoming EU elections. This exercise was part of the measures being implemented by the European Union[1] to ensure free and fair elections in May 2019.

A total of 80 players from 27 Member States, together with observers from the European Parliament, the European Commission and the ENISA, participated in this first EU table-top exercise (with the code name EU ELEx19) on the resilience of the upcoming European Parliament elections. The main responsibility for protecting the integrity of the elections lies with the Member States, and the overall objective of the exercise was to test and further strengthen their preparedness - especially their election and cybersecurity authorities – in the face of hybrid cyber-enabled threats, and to assess their ability to swiftly develop and maintain situational awareness at national and EU level if a serious cybersecurity incident which could impact on the integrity of the 2019 EU elections were to occur.

The exercise lasted a full day and was divided into three (3) sessions. In the first session, ENISA presented the Member States responses of a preparatory survey and each Member State then shortly presented the national picture. The second session was a table-top exercise where players were introduced into the exercise scenario and incidents. Players in the form of national teams, had to respond to a series of injects. In the third session, all the players' responses were presented and discussed.

This report is divided into three (3) sections. In the first section, a summary of the national briefings is presented while in the second the results of the preparatory survey are presented together with some key conclusions. In the third section, the exercise scenario is presented together with the various incidents, injects and main takeaways from the players' votes. Finally, in the Annexes we present anonymised responses to the injects and the satisfaction survey results.

[1] EC C(2018)5949 final

2. NATIONAL BRIEFINGS

Each of the 27 Member States provided a short overview of the steps taken in their country to shore up cybersecurity ahead of the upcoming elections and to mitigate possible threats.

Each Member State explained the setup of their national election cooperation networks and/or election security work stream, and elaborated on the level of multi-stakeholder and inter-departmental communication. Countries also highlighted the various measures taken ensuring the integrity of election data, protecting critical infrastructure, working with the private sector, preventing disinformation, and tackling hybrid threats.

With some variations between Member States, the measures taken included risk analyses, testing and troubleshooting, audits and certification, national exercises and simulations, penetration testing, escalation procedures, and the creation of real-time response units who will be on call during the election itself. While Estonia is the only Member State, which fully integrated the use of Internet in the elections process, the majority of the EU Member States integrate technology or digital solutions to some degree at varying stages of the electoral process (e.g. electronic voting, vote counting, and communication of results). To minimize possible disruption, paper or hard copy backup systems have been envisaged for the case an incident occurs. At the same time, all electronic procedures have paper trails records. Member States have also taken steps to ensure that any third-party service providers involved at any stage of the electoral process have been sufficiently trained/prepared.

Several Member States also highlighted their efforts to liaise with election authorities as well as political parties in order to ensure that they are adequately briefed on security issues, ensuring this way the prevention of disinformation spread, through dialogue with media and social media platforms.

In many Member States, the upcoming European Parliament elections take place in parallel with other elections processes – be it national, regional or local. As such, the exercise was welcomed by participants as an opportunity to review the steps taken to date and gain new experiences.

Speaking about needs identified through the preparatory work, many Member States expressed the need for greater transparency, openness and accountability, while others warned that fearmongering around the use of technology in election processes risk being just as damaging as any actual cyber-threat.

Other concerns expressed by some Member States were: the need to investigate the funding of political advertising online; outdated software or procedures; lack of formal procedures or ability to directly contact social media platforms.

3. PREPARATORY SURVEY

3.1 AIM

The preparatory survey aimed at mapping the preparation status of the players before the conduct of the exercise in order to identify gaps. For this, the NIS CG Compendium[2] and the EC recommendation on elections[3] have been used as a reference.

3.2 SETUP

The survey examined three (3) different aspects of cybersecurity, namely policies, capabilities and skills while an open question allowed the players to identify possible ways that the EU can further assist their efforts.

The surveys have been prepared and submitted before the exercise execution by the national single points of contacts of the national teams registered to play the exercise. The exercise organizers have emphasized the need to provide a coordinated response to this survey between all national players. Inputs were collected anonymously. Twenty-six (26) responses have been received in total.

3.3 SURVEY TAKEAWAYS

3.3.1 Policies

Regarding the applied cybersecurity policies, the picture presented by the Member States demonstrates that considerable efforts were taken. More specifically:

- Elections networks have been setup in the majority of Member States either fully or partly (21 out of 26)
- An analysis of potential risks has been performed by 23 Member States while only 2 Member States identified that they have not conducted a risk analysis at all. However, an important percentage, (38%) have not considered all relative stakeholders in their risk analysis.
- Most of the Member States (over 80%) identify critical infrastructures like telecom providers and energy providers as important and relevant stakeholders for the elections. Some Member States also consider the electoral registries as critical infrastructure.
- The vast majority of Member States include cybersecurity provisions in the Service Level Agreements (SLAs) with 3rd party providers. A substantial 34% goes one step further by including in the SLAs liability clauses for cybersecurity.
- Regarding business continuity in case of cyber attacks against the elections, an important 30% of the Member States says that although they have a business continuity plan in place, this has not been tested.
- Regarding the EU level coordination for the preparation of the elections, the large majority of the Member States (over 60%) says that they follow national policies, procedures and standards while the rest have a limited cooperation. In most of the cases however, the EC recommendation and the Compendium have been used as an aid for national planning.

3.3.2 Capabilities

The existence of adequate cybersecurity capabilities was the next topic in the survey. These include the horizon scanning for cyber threats, visibility over the network infrastructures used for

[2] Compendium on cyber security of election technology, CG publication 03/2018
[3] EC C(2018)5949 final

the elections, information exchange processes as well as aid to affected stakeholders. The conclusions here are the following:

- Although five (5) Member States say that they have not conducted horizon scanning for possible cyber threat vectors, the majority (over 76%) are doing it to some extent. Some Member States are now in the process of identifying possible threat vectors while four (4) say that although they have identified some threat vectors they have not taken specific measures for their protection. Eleven (11) Member States have done the extra mile to proactively monitor possible threats.
- The national CSIRTs play a role in the elections process for fifteen (15) Member States and in eight (8) cases national CSIRTs have monitoring access to election networks and capabilities. Some Member States say that in the case of Federal Member States, the role of the national CSIRT is limited regarding the elections while a few others say that it is not in the national CSIRT mandate to deal with elections.
- Regarding the EU collaboration, ten (10) Member States are already using the CSIRTs network as a vehicle while the rest agree that the CSIRTs network should be used for collaboration regarding the elections.
- Finally, the vast majority (over 80%) is taking measures towards the protection of election stakeholders, mainly politicians and political parties. An important 42% is doing this in a proactive way by providing relevant protection measures.

3.3.3 Skills

The existence of adequate skills among election stakeholders is often considered as a less important factor and one may argue that this is also reflected in the results of this section. It is however perhaps the most important one. Skills include both cybersecurity competencies across all levels of administration and general public awareness. The main takeaways here are the following:

- Half of the Member States have implemented a cybersecurity education program for relevant stakeholders, fully or partly. Five (5) Member States do not have a cybersecurity education program in place.
- National cybersecurity authorities took an active role towards the briefing of election stakeholders for cybersecurity concerns for 70% of the Member States. However, these briefings have been conducted across all levels of administration, from political to technical by only seven (7) Member States.
- Regarding the existence of cyber awareness campaigns, six (6) Member States are systematically conducting such campaigns while eleven (11) other have done it ad hoc once or twice in the last year. However, six (6) Member States have not conducted at all such campaigns.
- For the EU wide cooperation regarding awareness, in twelve (12) cases there has been some briefings while five (5) Member States say that they need more. An important 38% however did not have briefings with EU institutions.

4. TABLE TOP EXERCISE

4.1 EUELEX19 SCENARIO

The EUELEx19 scenario contained a Road to crisis and a total of eight (8) incidents. The road to crisis was starting from the beginning of 2019 going up to a week before the EU elections. The scenario described a multi-vectored campaign including public opinion manipulation, confidentiality attacks against EU institutions as well as integrity and availability attacks against elections infrastructures and data. In order to stimulate the situational awareness of the audience, the initial attacks seemed not to be related to the elections themselves however as it proved through the various incidents, there has been a direct orchestration of all attacks by a single, well-resourced malicious actor.

4.1.1 Road to Crisis

In January 2019, media shared reports of a supply chain attack against ‘GearX’, a major non-EU manufacturer of networking gear such as Routers, Network Switches and Servers. Over the past 10 years, this manufacturer appears to have sold a significant amount of Internet backbone gear to EU Member States, ISPs and Telecom Operators. The media reports emphasize the risk of eavesdropping, man in the middle attacks and exfiltration of information using specific backdoors in those systems. The reports also point out a potential negative impact on banking transactions, and the risk of mobile phone data being ex-filtrated. The network gear manufacturer strongly denies these reports, accusing a rival EU manufacturer of driving them. On 10 February, INTCEN notifies the EEAS and the Commission that a few dozen groups have appeared on social media almost simultaneously, calling for EU citizens to protest about user information privacy in EU cyber space. Intelligence information reveals that these cyber personas are in fact trolls, managed and directed centrally.

By mid-February, these groups have grown significantly, with some organizing limited protests in certain EU countries. These events are combined with street concerts in order to attract more people. The prevailing messages are critical of traditional media, newspapers and TV channels for allegedly keeping the truth about data privacy from EU citizens.

On 31 March, the “Free Speech in Europe” movement organizes simultaneous protests in several EU capitals. They are calling for EU citizens’ privacy rights to be protected and accuse Member States and EU authorities of doing nothing to ensure this happens. According to National Authorities the protesters are mainly young people. No damages or injuries are reported. On 15 April, a large non-EU nation bans public procurement of equipment from ‘GearX’. This triggers a new wave of protests across Europe, led by the previously active social media activist groups. Political parties and candidates, are raising concerns around the integrity of EU elections. EU politicians join many of the social media groups driving this activism.

4.1.2 Incidents

In this section, the different incidents that were given to the players are presented along with the corresponding questions that were posed for polling. A more detailed view of the players' replies are presented in Annex A.

4.1.2.1 Incident 1

In several EU countries, the DNS servers of ISPs and Telecom companies experience a DNS poisoning attack on their local cache registries. The DNS poisoning specifically affects the DNS entries for 'EU Institution X' and 'EU Institution Y' websites, but initially goes unnoticed. Soon after, a series of phishing emails purportedly from the Executive Directors of 'EU Institution X' and 'EU Institution Y'' redirect recipients – employees of those institutions – to perfect replica websites of those EU Institutions' intranets. Because of the DNS poisoning, the redirect addresses are identical to the original address of the EU Institutions' intranets, with the sole difference that they ask employees to re-authenticate their credentials.

Takeaway 1

Correct situational awareness reflections. More information was asked in order to have a concrete assessment.

1. How would you define the situation?
2. Could this incident potentially impact the upcoming EU elections?

4.1.2.2 Incident 2

A preliminary investigation of the previous incident reveals that the malicious websites and methods are associated with APT XX, a criminal group likely linked to a non-EU state that is believed to have funded previous cyber operations against EU and US governmental bodies, industries and banks. CERT EU issues a warning to EU bodies, institutions and the CSIRTs network about possible escalation of cyber offensive operations in the coming days.

1. Is this purely an EU matter, with implications for the EU institutions?
2. Should appropriate National cyber authorities warn National election authorities of the increased possibility of offensive cyber operations?

Takeaway 2

The need for situational awareness is well understood by the players.

4.1.2.3 Incident 3

A European cybersecurity researcher is reporting that detailed records of EU residents – but non-EU voters – have been found on the Dark Web following from the two EUI data breaches. These include names, addresses, phone and social security numbers, dates, place of birth and more. The total number of confirmed ex-filtrated records exceeds 60,000 entries. The researcher also reports that the Dark Web repository has been used by APT XX in the past. Social media groups share this information, blaming the EU and national governments for not protecting EU residents' personal data.

Takeaway 3

Players remained neutral but maintained situational awareness.

1. How would you react to this event?
2. How would you react to increased public pressure and mistrust?

4.1.2.4 Incident 4

In several EU Member States, a series of spear-phishing campaigns targets Election Networks and subcontractors dealing with the elections. In your country, the spear-phishing emails are supposedly sent by National Political authorities (Minister’s secretary general) and the European Parliament. The emails ask victims to report on the National election security readiness and any increased security measures been undertaken to ensure the safety of election infrastructures. These emails specifically refer to the recent cyber attacks and to an “EU checklist of best practices” shared as an attached pdf form. The checklist is supposedly based on the NIS Cooperation Group ‘Compendium on Cyber Security of Election Technology’ endorsed by the MS in 2018. The malicious attachment is opened by several recipients and exfiltrates admin access credentials from your national registry of voters.

Takeaway 4

Players correctly assessed that the incident has EU wide dimensions. However opinions are divided whether information should be disseminated to EU Institutions or not.

1. Is this purely a National matter?
2. What would be your National reaction?

4.1.2.5 Incident 5

Your Cybersecurity Authorities discover a hacked copy of the EP Crypto tool on the dark web. The tool has been engineered and is found to contain a data modification capability. The tool also seems to have a backdoor ‘beacon’ function, communicating with a Command and Control server associated with APT XX. Upon this discovery, your Cybersecurity authority immediately informs your National Elections Authority.

1. How would your reaction be?

Takeaway 5

Players correctly assessed that EU level should be informed about the hacked crypto tool.

4.1.2.6 Incident 6

The discovery of the compromised tool is leaked to the media. TV channels, Newspapers, and Social Media put pressure on the EU and National authorities, raising concerns about the integrity of the EU elections. The 'suspicious' social media groups, already identified in February, publish fake information regarding the extent of the hack, claiming that Member States are using a hacked tool to relay compromised voter data.

1. How would your reaction be?
2. How would you respond to media pressure and queries?
3. How would you respond to the fake news campaign?

Takeaway 6

The majority prefers a neutral handling of the media but at the same time take all necessary measures by implementing business continuity plans. Fake news mitigation is considered as a multi vectored effort including Social media platforms, the EU and National legal authorities.

4.1.2.7 Incident 7

Following recent developments, the European Parliament, the European Commission's DG JUST and several Member States recommend an immediate verification crosscheck of voter registries. The checks reveal that many MS voter registries are contaminated with data from the ex-filtrated lists from 'EU Institution X' and 'EU Institution Y'. The checks also reveal duplicate entries of the same individuals in multiple Member States and the additions of EU residents but non-EU voters. Over 20,000 illegitimate and duplicate entries are eventually discovered across the EU."

1. What number of illegitimate entries across the EU would be deemed to pose a threat to the electoral process?
2. Do you think that a total of 20,000 illegitimate and duplicate entries (across the whole EU) poses a threat to the credibility of the elections' outcome?
3. Do you think that the elections should be postponed?

Takeaway 7

Various views on the numeric threshold that can qualify a threat as critical. The reputational risk is considered critical by most of the players.

4.1.2.8 Incident 8

Just two hours after the polls open, a massive Distributed Denial of Service (DDoS) attack and website defacement hit the election network and media channels across the EU. This results in extensive outages of government and media websites, as well as publishing of fake results on hijacked web pages. The attacks last approximately 45 minutes. In addition, two major EU telecom providers inform the election network that SS7 attacks are reported in telephony networks (cell phone/SMS hi jacking), potentially affecting official cell phones.

1. How would you react?
2. If such incidents are reported in your country, would you immediately engage with the relevant EU entities?
3. Following the outages, media are asking the government for more information. The government spokesperson has asked you for a statement they can share. What line would you take?
4. The media is approaching you directly, asking for more information. What would you do?

Takeaway 8

Mature incident handling. Players realise that panic of the public is serving the attackers' purposes. A difference in opinions whether the EU institutions should only be aware or they should have an active role by providing support.

5. CONCLUSIONS

The European Commission recommendation and the Compendium on Cyber Security of Election Technology appeared having played a significant role not only as a reference for national preparations but even for threat identification.

Majority of Member States have managed to assemble national teams composed of different stakeholders (e.g. cybersecurity authorities, electoral authorities, CSIRTs) involved in the EU elections which contributed to their ability to provide comprehensive responses. Overall, the training audience demonstrated maturity in their responses during the exercise. For instance, there was clear awareness that the impact of serious cyber incidents extends beyond the technical dimension and affects the political level of decision making as well as the society itself.

When it comes to the organisation of elections, timing is key. This is why some players stated that such efforts should have started earlier. At the same time, election security is a continuous process and therefore national efforts will have to go beyond the European Elections of May 2019, with a view to securing future national and local elections.

Overall, the exercise revealed a considerable degree of awareness of how to handle multi vectored cyber-attacks by the Member States.

Nevertheless, some Member States who have not completed implementation of measures foreseen in the Commission Recommendation on free and fair elections should do so in the run up to the elections. This includes notably:

- Establishing a national election cooperation network and extending the scope of the network to other relevant policy issues, such as disinformation;

- Setting-up dedicated communication tools or procedures;

- Defining an incident response plan applicable to cyber-enabled incidents or attacks against democratic processes and testing it through national level exercise. For members having already an incident response plan, this could be revised based on lessons learnt during EU ELEx19.

Moreover, the exercise showed that there are a number of areas for improvement, where Member States and institutions can jointly work towards increasing cyber-resilience of electoral processes across the EU. This includes:

i) Improve risk management processes.

a. Action which could be taken in the short term (before the EU elections) are:

- Completing the horizon scanning for threats to elections including reputational risks attached to disinformation campaigns;
- Taking the necessary security measures mitigating top threats. In particular, review and if necessary revise provisions related to cybersecurity in Service Level Agreements (SLAs).

b. Action which could be taken in the long term (after the EU elections) are:
- Performing of a coordinated EU-level threat scanning and analysis of common risks;
- Developing of standard EU cybersecurity requirements for SLAs with third party providers of services related to the elections;
- Defining thresholds to asses when a state of crisis should be declared.

ii)*More structured approach to awareness raising and training*.

a. Action which could be taken in the short term (before the EU elections) are:
- Establishing of a support desk providing technical support to relevant third parties (political parties, foundations and campaign organisations);
- Conducting cybersecurity briefings for relevant government bodies and political parties (both political and administrative level).

b. Action which could be taken in the long term (after the EU elections) are:
- EU level coordination and support to national awareness raising programmes;
- Developing of dedicated training activities for relevant third parties as well as electoral authorities.

iii) *A stronger role for CSIRTs in the election process.*

a. Action which could be taken in the short term (before the EU elections) are:
-Guaranteeing that the national CSIRT can monitor relevant networks/capabilities/tools in the run-up to the elections;
- Including the national CSIRT in the national election cooperation network.

b. Action which could be taken in the long term (after the EU elections) are:
- Enhancing the level of technical capabilities allowing for an effective scanning of threats as well as adequate emergency response.

iv) *Closer EU level collaboration and information sharing.*

a. Action which could be taken in the short term (before the EU elections) are:
- Making use of the CSIRTs Network to share threat intelligence in the run-up to the elections and ensure that the relevant information reaches the national election cooperation network.

b. Action which could be taken in the long term (after the EU elections) are:
- Organising shared meetings and/or exercises gathering the Cooperation Group and EU level election cooperation network;
- Integrating the national election cooperation network in the Blueprint framework for crisis response by defining national roles and procedures at operational level as well as identifying common standard operating procedures for information exchange;
- Ensuring a more structured and continuous sharing of information regarding cyber enabled threats and incidents through dedicated tools.

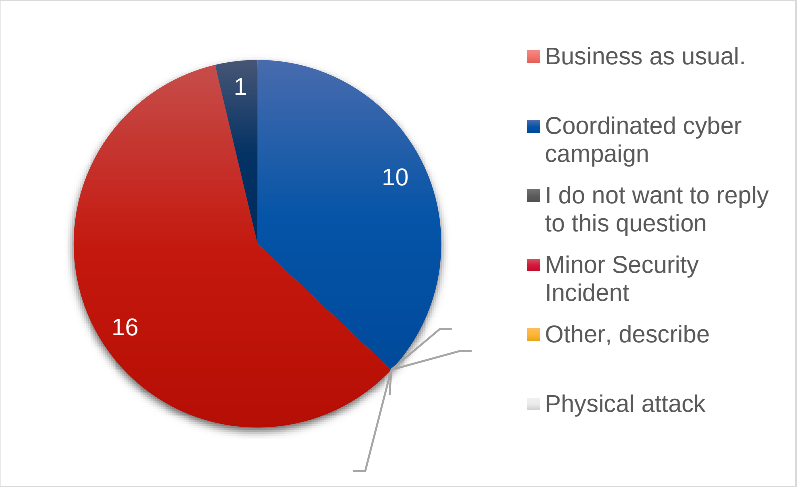
Lessons learnt should be shared in a meeting taking stock of the European elections, this could be done in the context of the EU level election cooperation network. Moreover, this discussion should be reflected in an updated version of the Cooperation Group compendium.

EUELEx19 can be considered as a successful event. The training audience feedback have been positive for the EUELEx19 conduct, scenario, organization and most of the players believed that the exercise added value to their national efforts for safer EU elections. This is reflected in the players' feedback, which are presented in Annex B.

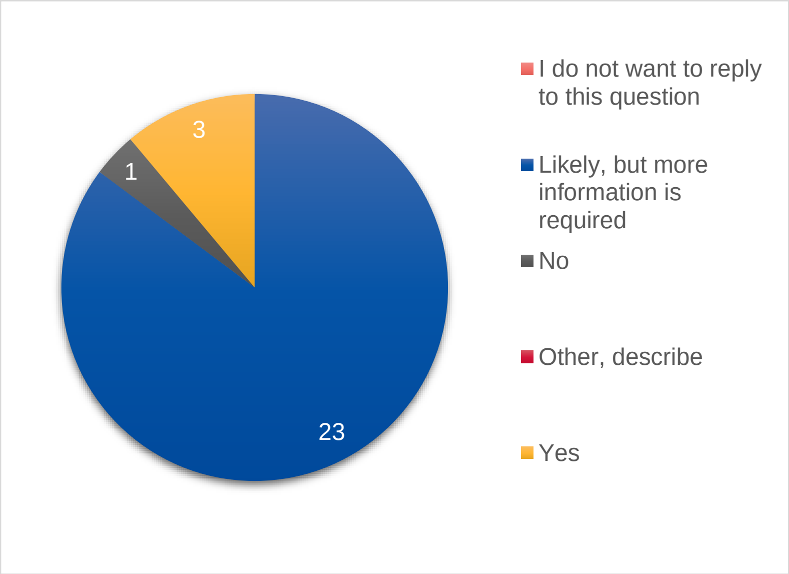
ANNEX A INCIDENTS RESPONSES:

A.1 INCIDENT 1

Question 1.1: How would you define the situation?

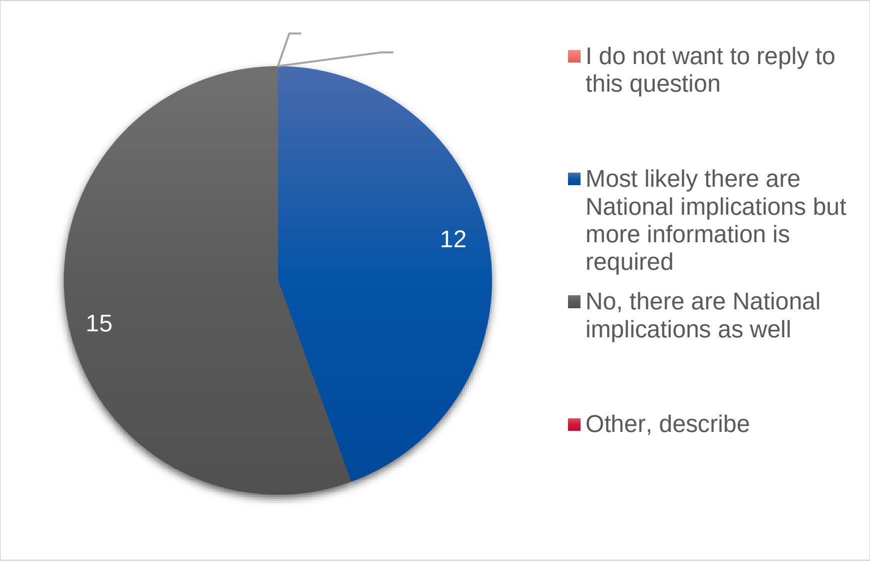


Question 1.2: Could this incident potentially impact the upcoming EU elections?

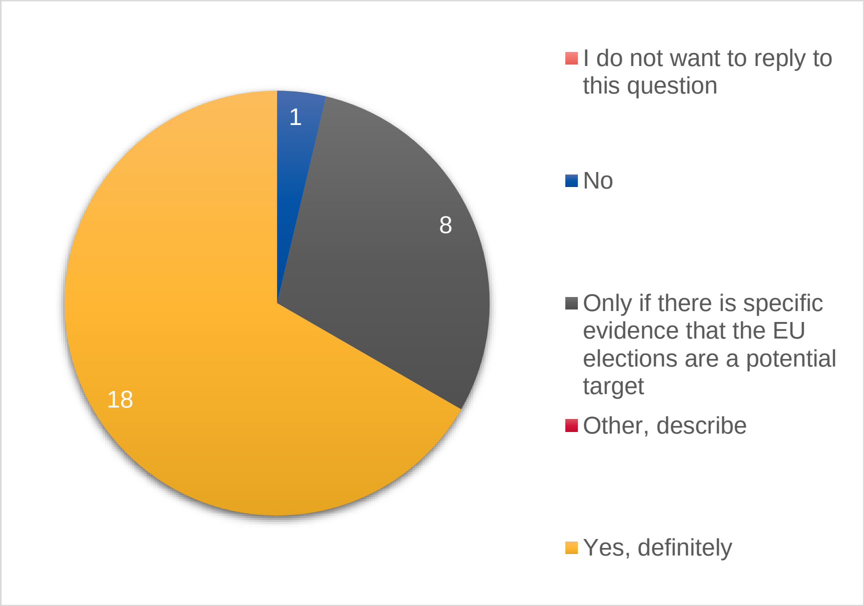


A.2 INCIDENT 2

Question 2.1: Is this purely an EU matter, with implications for the EU institutions?

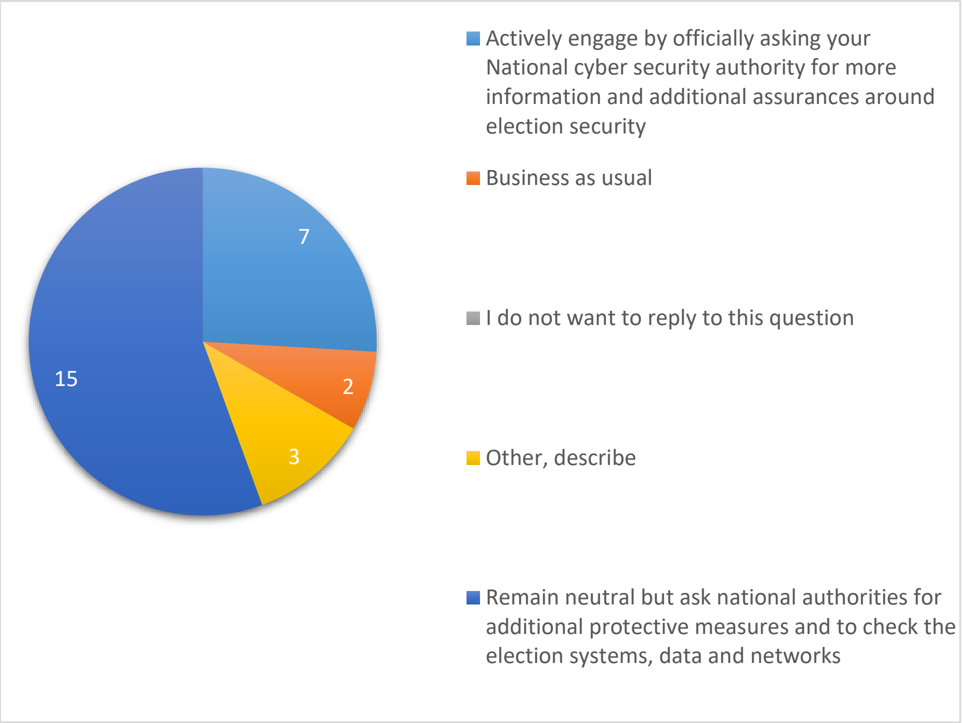


Question 2.2: Should appropriate National cyber authorities warn National election authorities of the increased possibility of offensive cyber operations?



A.3 INCIDENT 3

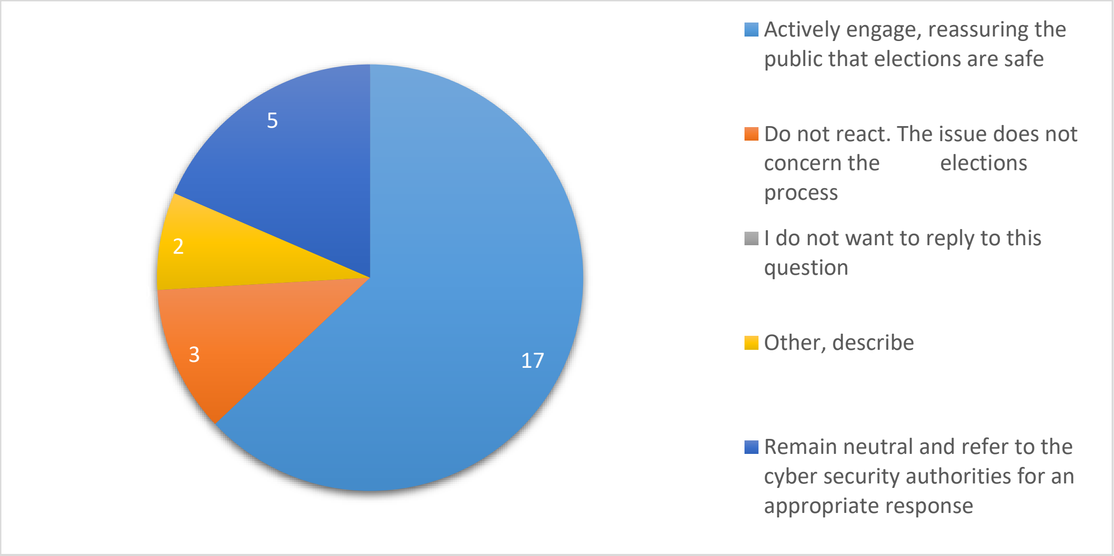
Question 3.1: How would you react to this event?



Other/describe

- Electoral authorities would remain neutral but ask National authorities for additional measures. National cyber security would enhance the monitoring process.
- Liaise with data protections authorities to check for any reports of data breaches.
- The incident is serious but does not seem relevant for election. Does not come from an election register.

Question 3.2: How would you react to increased public pressure and mistrust?

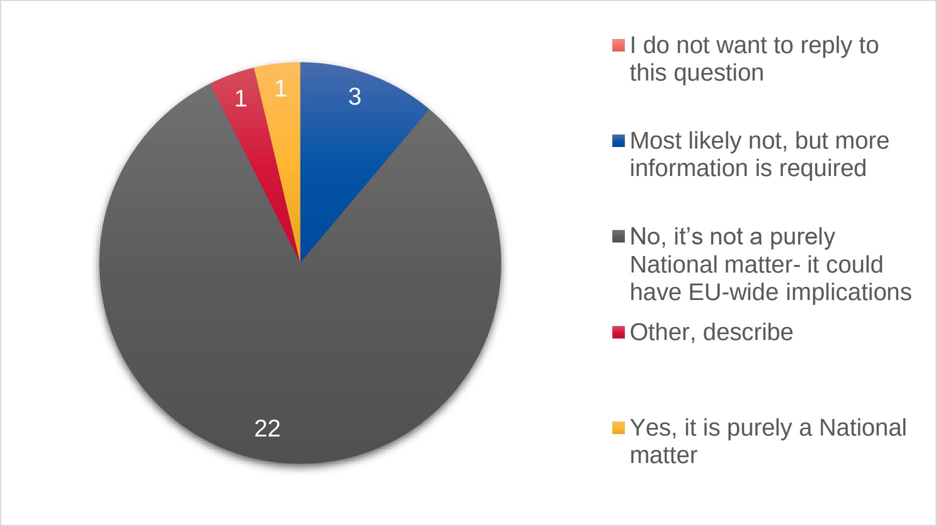


Other/describe

- Combined appropriate response from election authority and cyber security agencies. Necessary communication processes should be prepared in advance.
- Answer A plus need to find out more about the data before we can accurately say that elections are safe. Assure public that all institutions are engaged in investigation.

A.4 INCIDENT 4

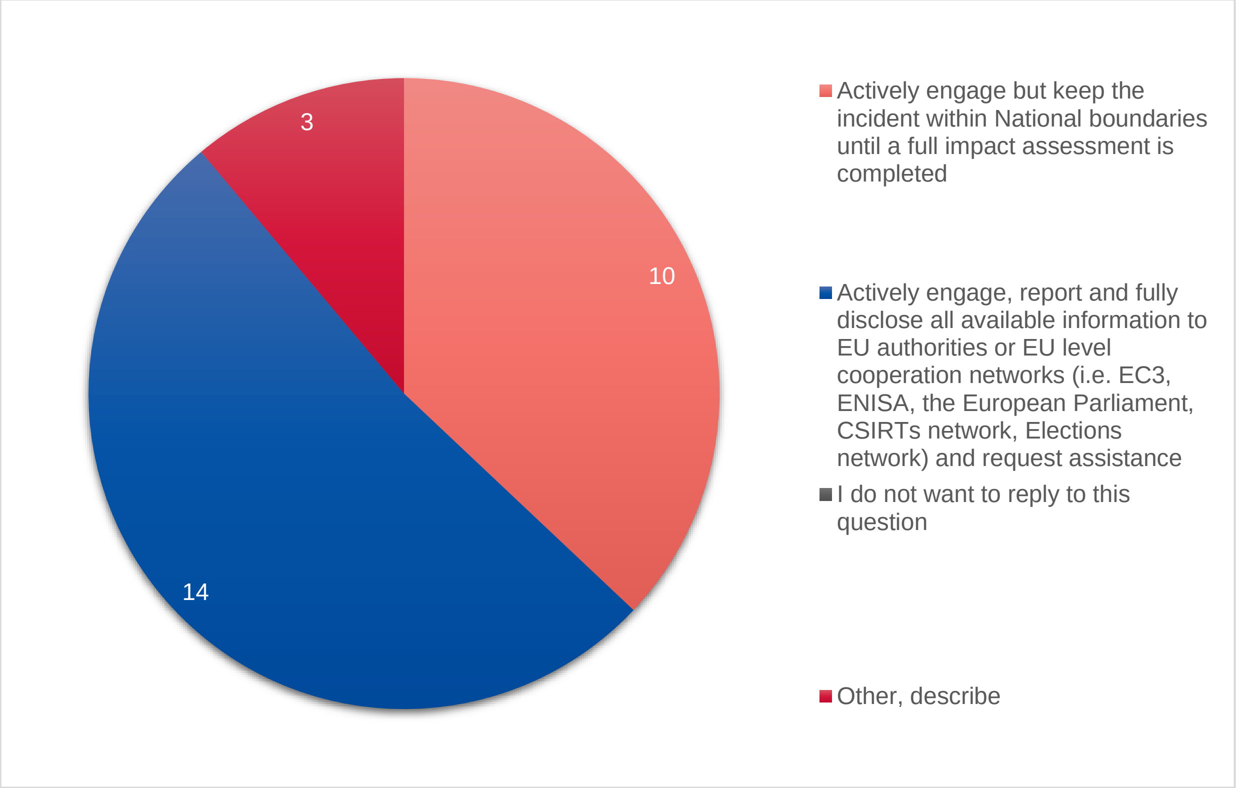
Question 4.1: Is this purely a National matter?



Other/describe

- It’s not a purely National matter, it would have EU implications but the scenario is not realistic. In our country no admin credentials for National registry are obtainable in this way.

Question 4.2: What would be your National reaction?

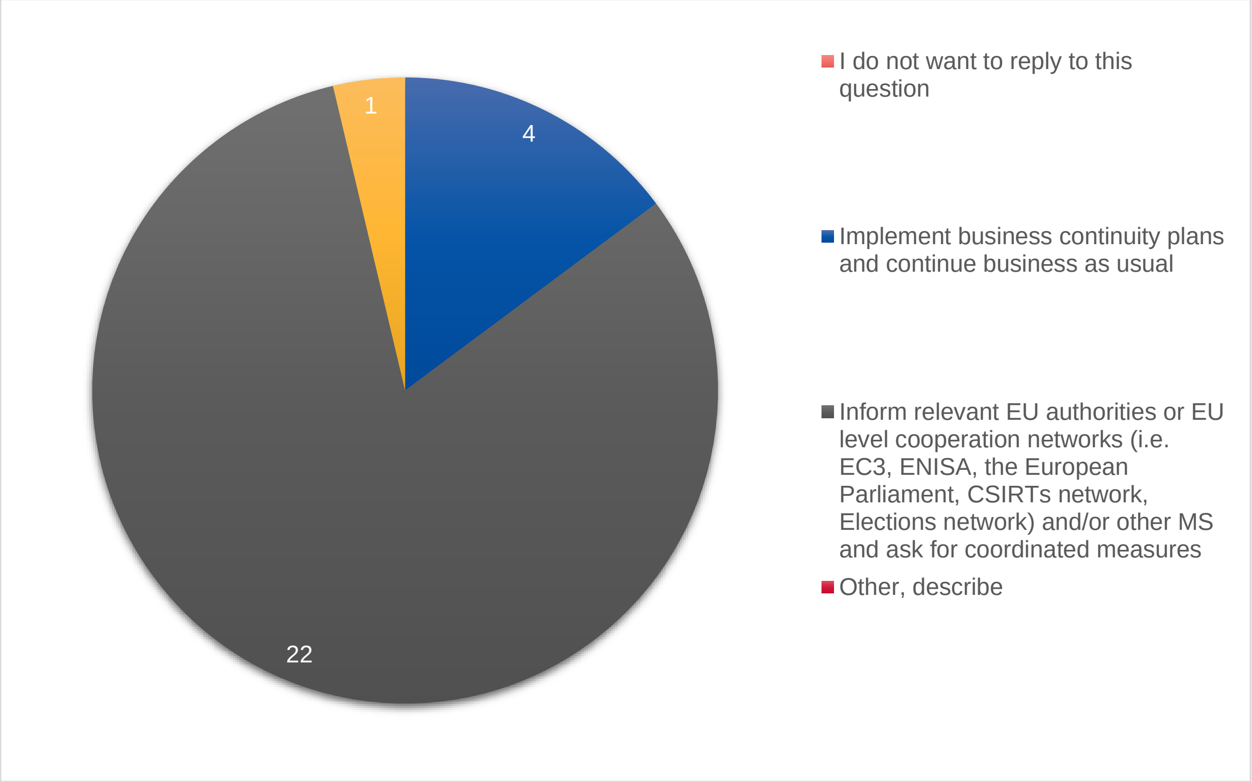


Other/describe

- It is B but there would be cooperation at technical level (and technical information sharing) between the National cyber security authority and the CSIRTs network.
- Answer A, but only relevant (not all) information with selected authorities and networks (CSIRT,…)
- The information is appropriately shared with EU institutions, if implications with other EU MS and/or EU institutions are determined (We would not share full information)

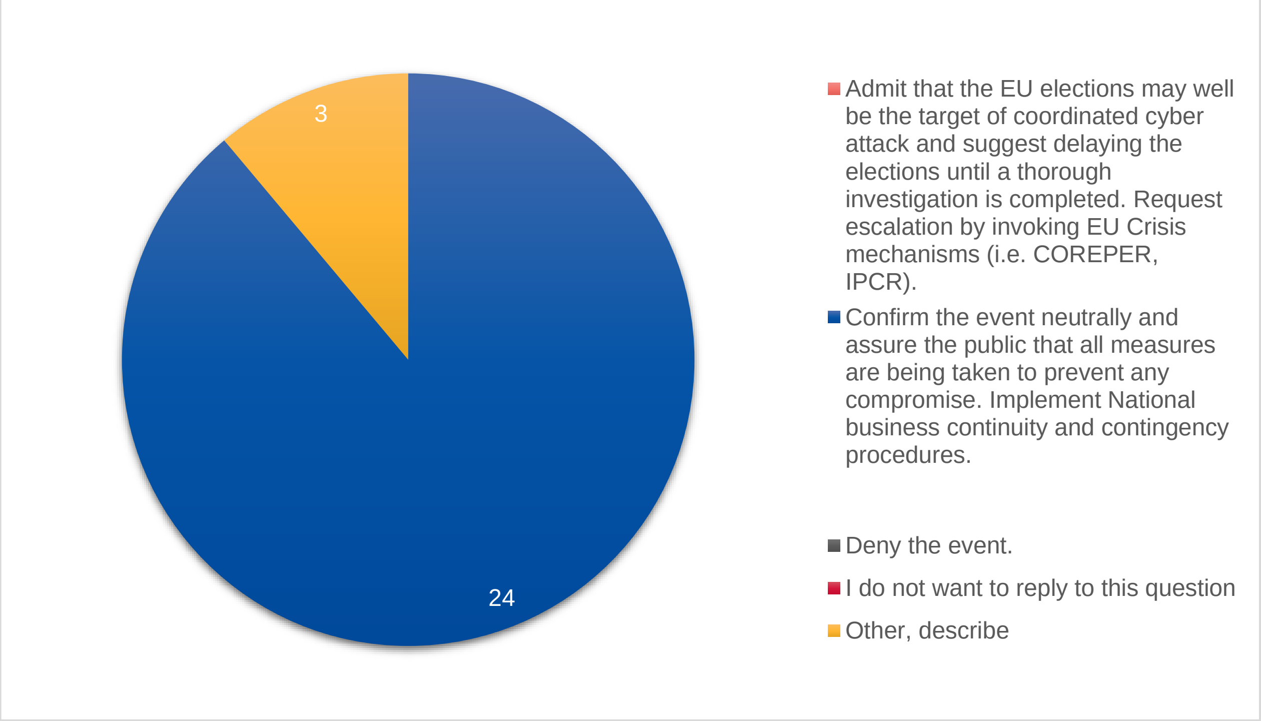
A.5 INCIDENT 5

Question 5.1: How would your reaction be?



A.6 INCIDENT 6

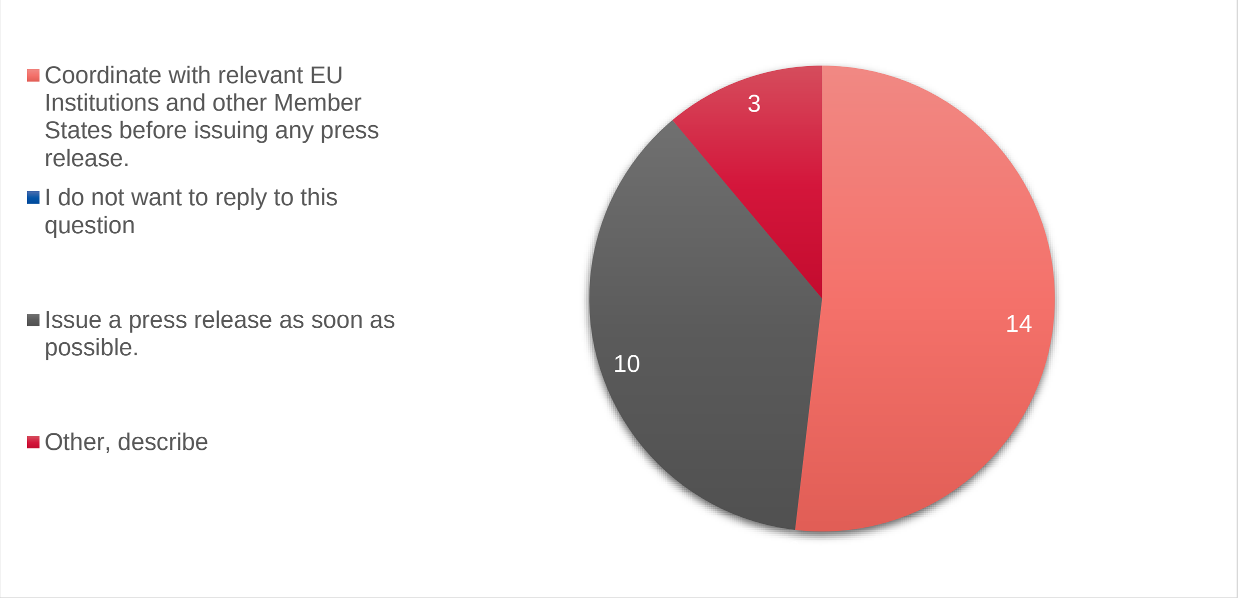
Question 6.1: How would your reaction be?



Other/describe

- Answer B plus clarification to the public (coordinated with social media providers and media institutions) regarding the fake news. Tell the truth.
- Answer B but assuming that the situation is under control and has no effect on integrity of election.
- Confirm the event neutrally and assure the public that all measures are being taken to prevent any compromise. Activate National business continuity and contingency procedures. Inform EU institutions if necessary.

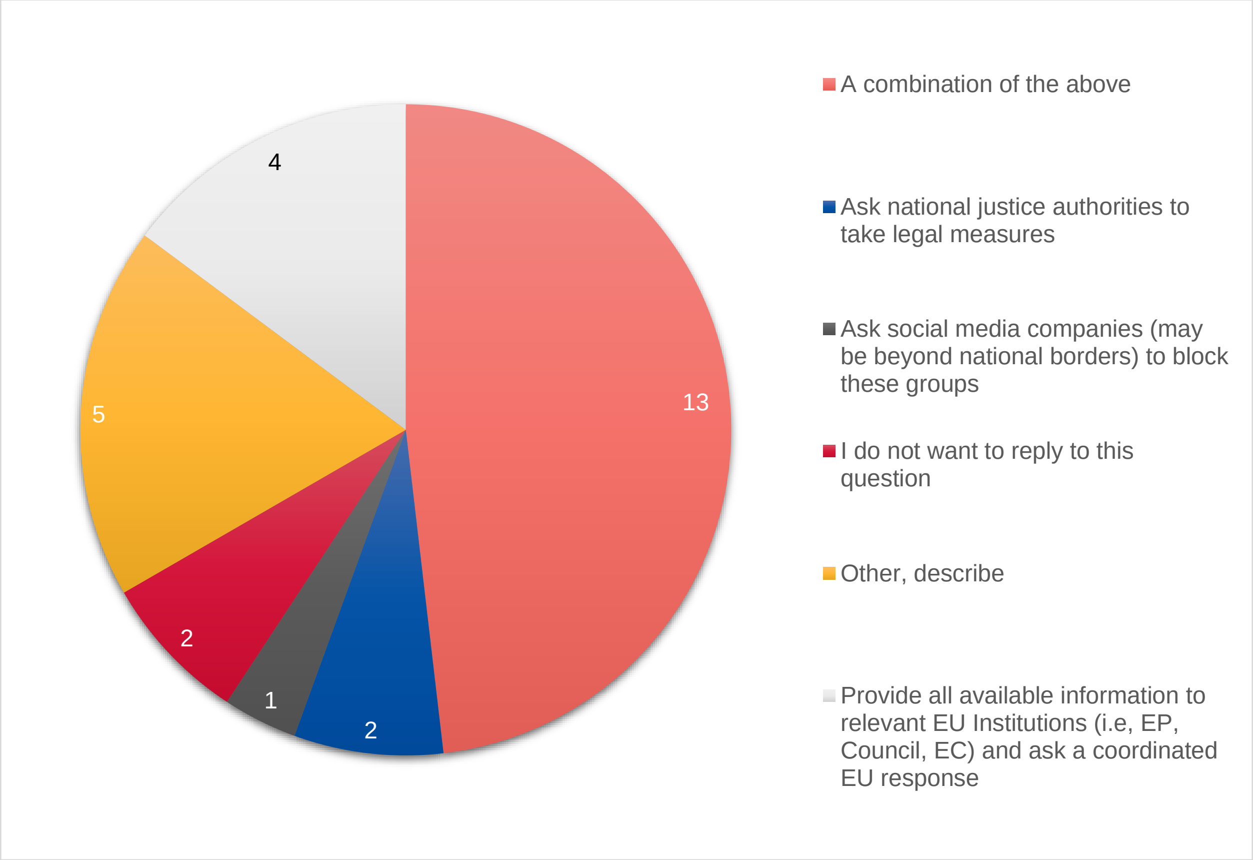
Question 6.2: How would you respond to media pressure and queries?



Other/describe

- It demands a quiet and coordinated press release with highest possible consensus with EU authorities.
- We will issue the press release immediately, because we are also running National elections. At the same time we accept and will cooperate for an EU coordinated press release concerning the EU elections.
- Issue a press release as soon as possible and inform EU partners

Question 6.3: How would you respond to the fake news campaign?

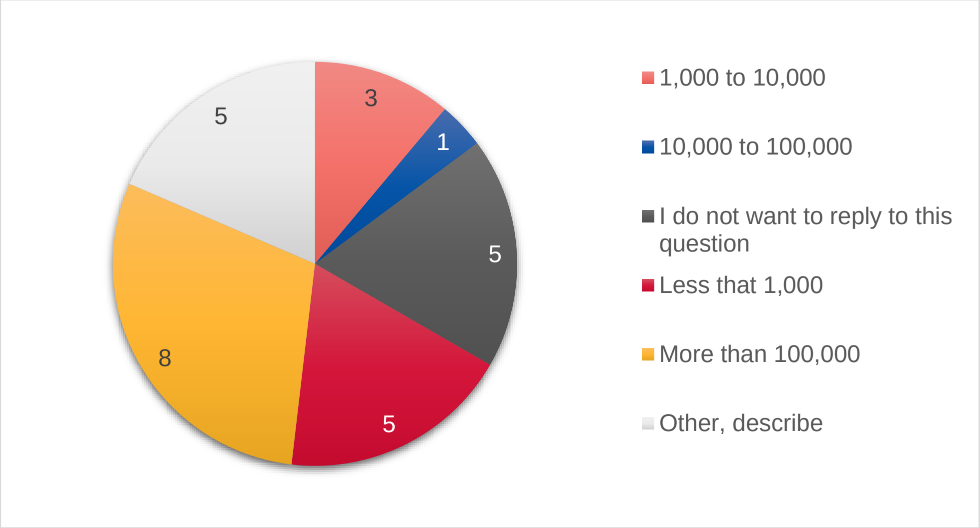


Other/Describe

- Both B & C, but we would not ask the social media companies to block the campaign but ask them to check if it is in violation of their user policy
- Activating fake-news debunkers group/volunteers. Block the group. Ask Police fake-news unit to act
- Combination of B & C. Ask social media companies to block these groups. Provide all relevant information.
- Inform internal 'rapid alert system'. Engage with social media companies on the authentic behaviour. Inform National cooperation network, Ministry of Justice is part of that network.
- Answer C plus cooperation among different authorities to emphasize correct information in strategic communication.

A.7 INCIDENT 7

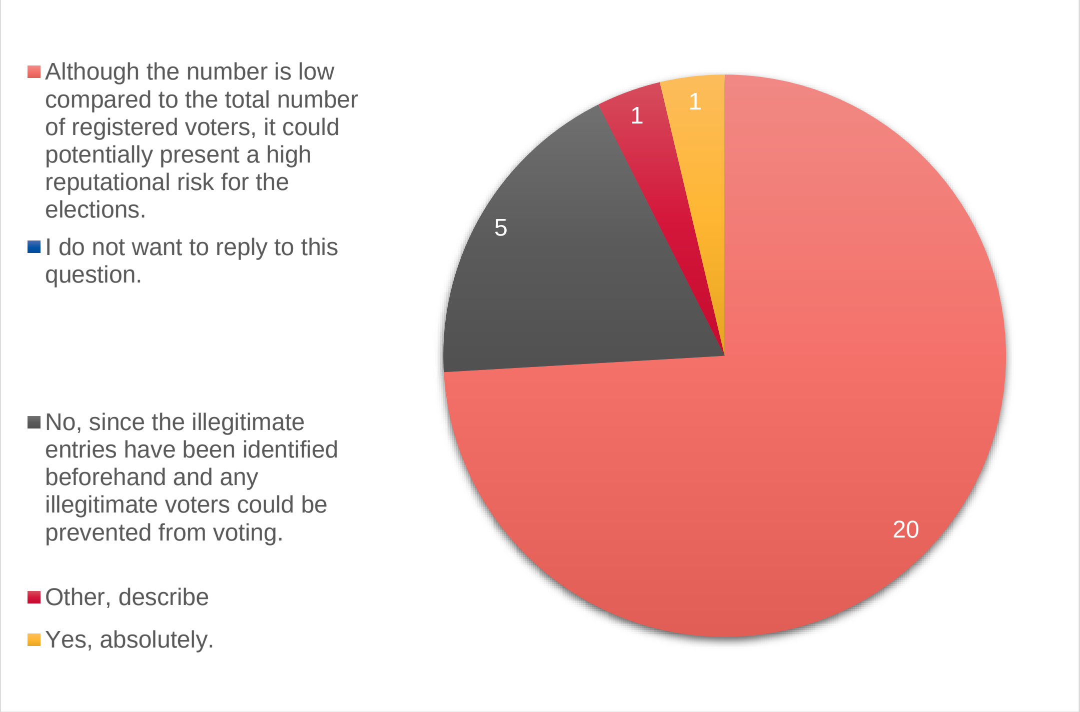
Question 7.1: What number of illegitimate entries across the EU would be deemed to pose a threat to the electoral process?



Other/describe

- Not relevant scenario
- None of the above
- Any number of illegitimate entries would be a threat.
- Question can only be answered when knowing the actual outcome of election and how narrowly a seat has been achieved (or not).
- Not a relevant scenario. Depends on which MS are affected and how the crypto tool is used.

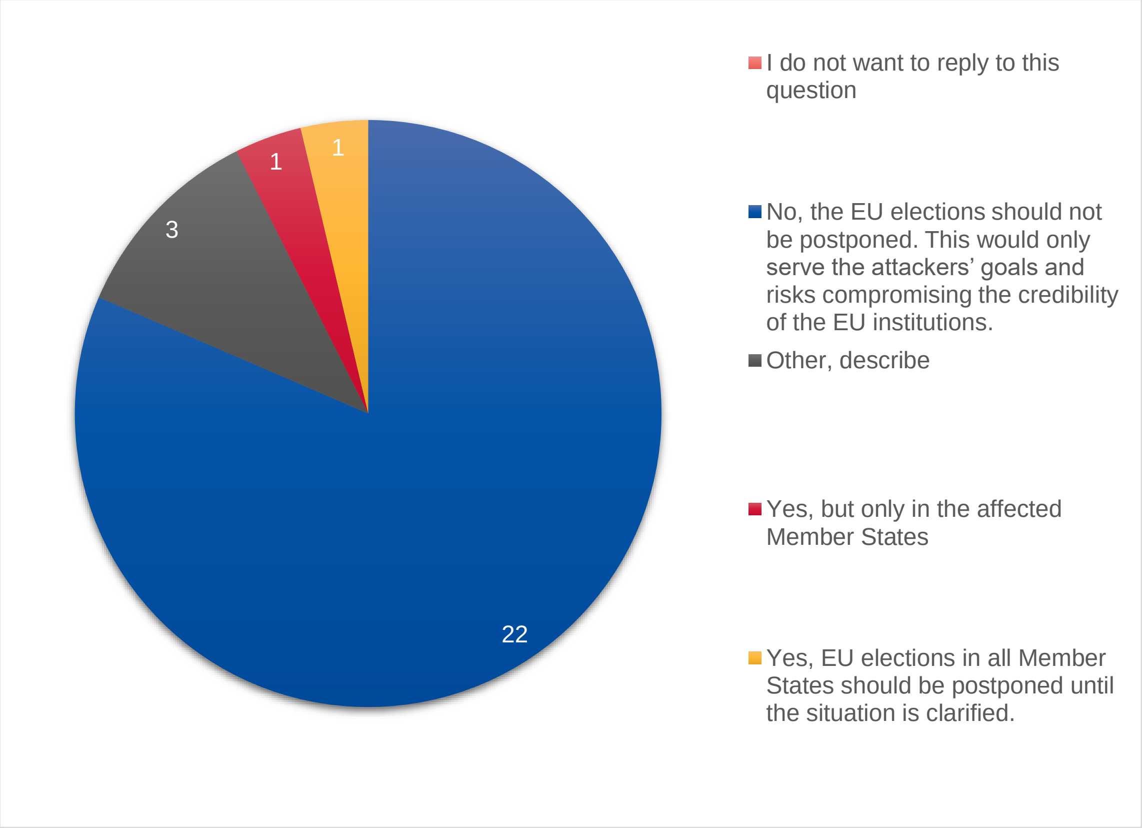
Question 7.2: Do you think that a total of 20,000 illegitimate and duplicate entries (across the whole EU) poses a threat to the credibility of the elections' outcome?



Other/describe

- Not relevant scenario. Registers are published 20 days before the poll. Corruptions should have been identified at that time and not 2 days before.

Question 7.3: Do you think that the elections should be postponed?

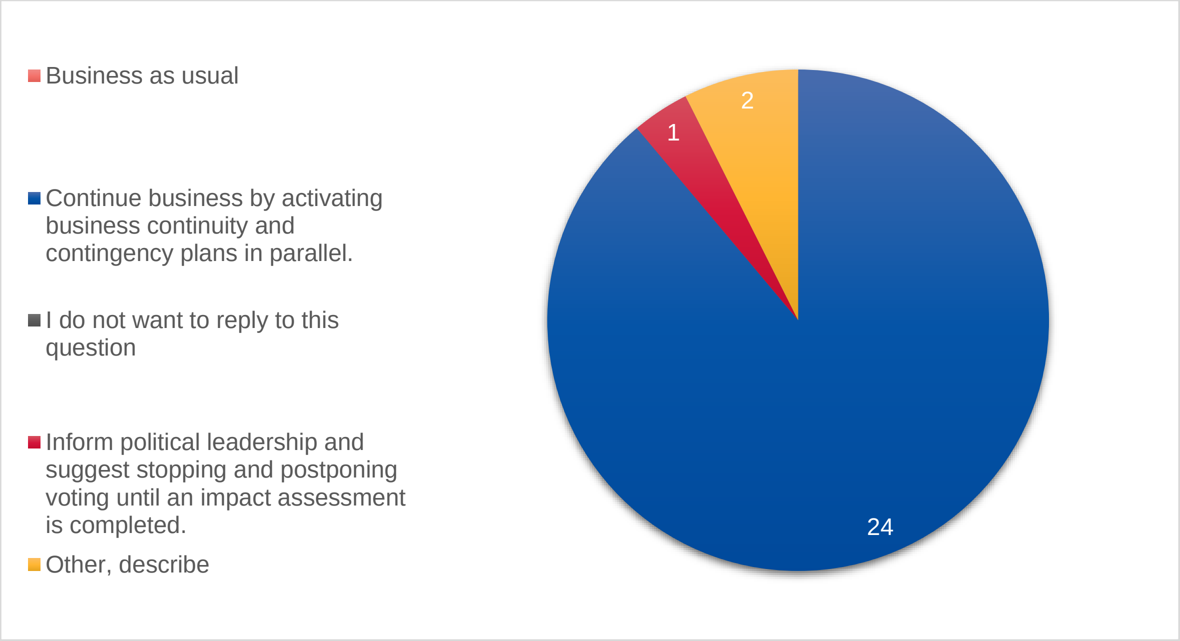


Other/describe

- Elections should not be postponed
- No, it should not be postponed, particularly as there is no legal basis to do so 2 days before the election.
- It's not possible to postpone elections at this stage. The date is bound by law. In addition, postponing would serve the attackers' goals.

A.8 INCIDENT 8

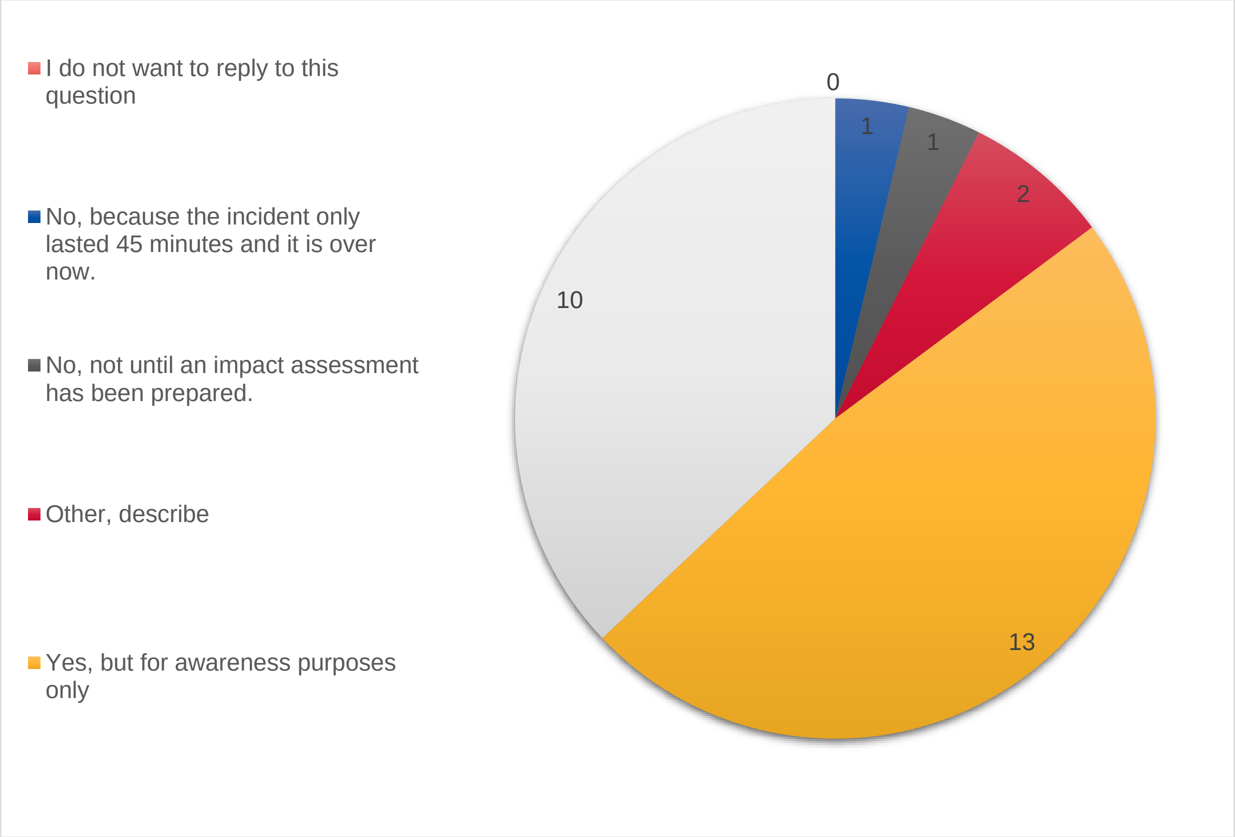
Question 8.1: How would you react?



Other/describe

- A combination of B & C is necessary because political leadership is crucial in this moment.
- We will continue and will start the backup plan (Paper voting/ Attack against hackers/ block all activity abroad)

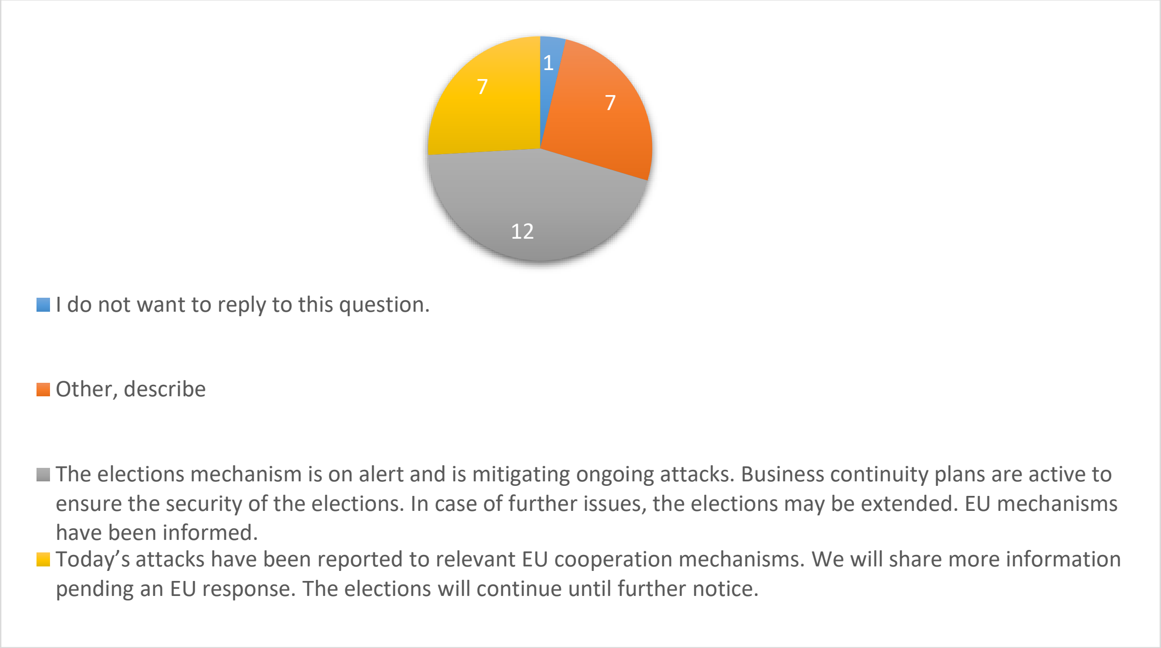
Question 8.2: If such incidents are reported in your country, would you immediately engage with the relevant EU entities?



Other/describe

- C but with informal discussion
- Answer D but without ‘asking for support’, because the technical measures are under National responsibility.

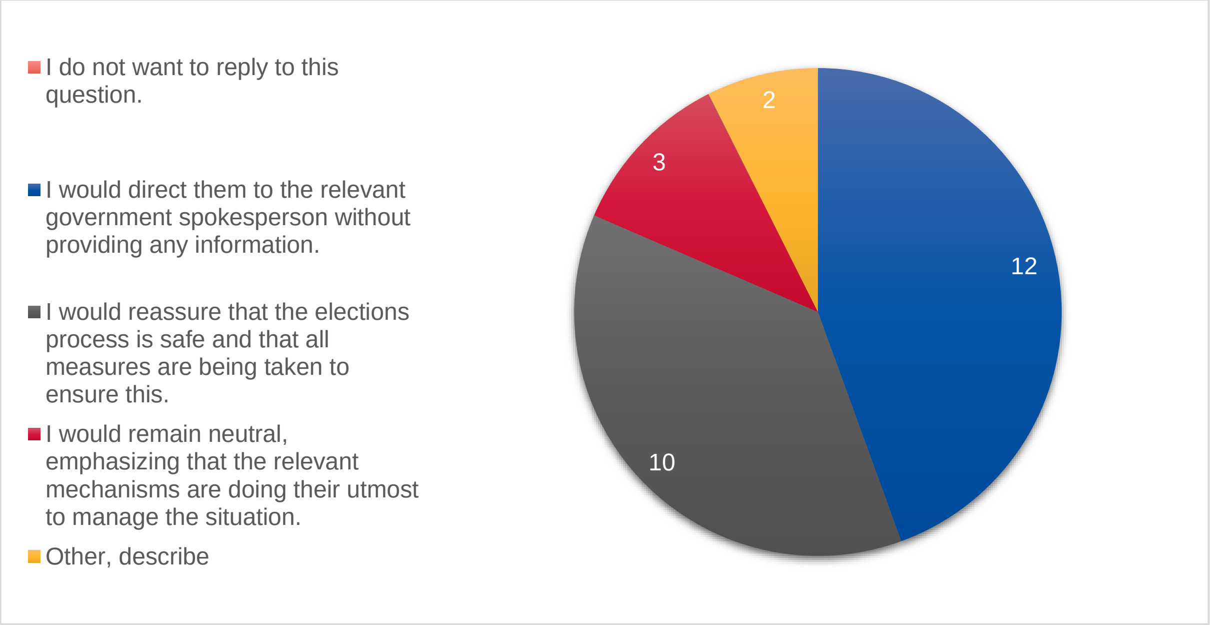
Question 8.3: Following the outages, media are asking the government for more information. The government spokesperson has asked you for a statement they can share. What line would you take?



Other/Describe:

- We would go for C but without the last sentence. Our message will be that the elections will continue
- A very calm press release from elections authority and cyber authority.
- Option B without the possibility of elections being extended as legal regulation does not allow for it.
- Communication focus on the resilience of the electoral process.
- Answer C plus informing that relevant National cooperation mechanisms are in place and ensuring the security of elections at National level.
- Attacks have been reported (answer C) but elections continue until further notice.
  The authorities are aware that a cyber incident is targeting at different actors. Elections are ongoing and voting takes place according to normal procedures. Relevant authorities are working to mitigate the problem.

Question 8.4: The media is approaching you directly, asking for more information. What would you do?



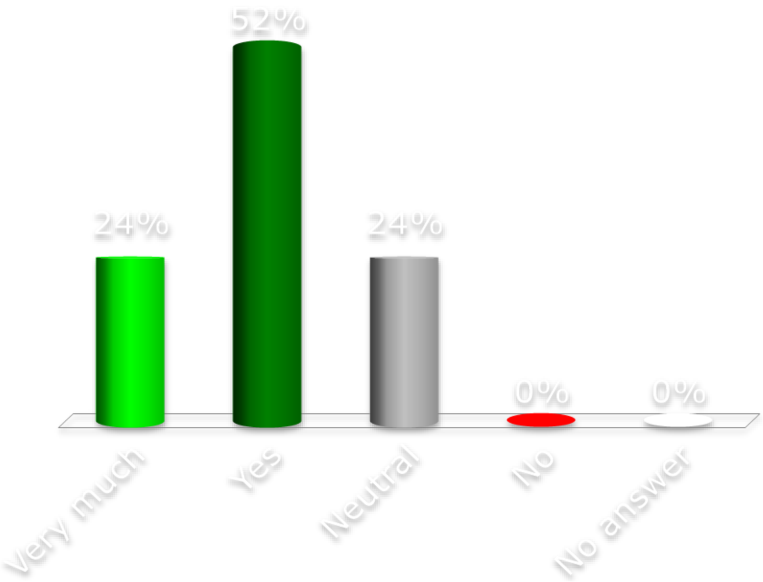
Other/describe

- After conferring with the relevant top authorities, media representatives, a decision about the appropriate reaction would be taken.

ANNEX B: SATISFACTION SURVEY

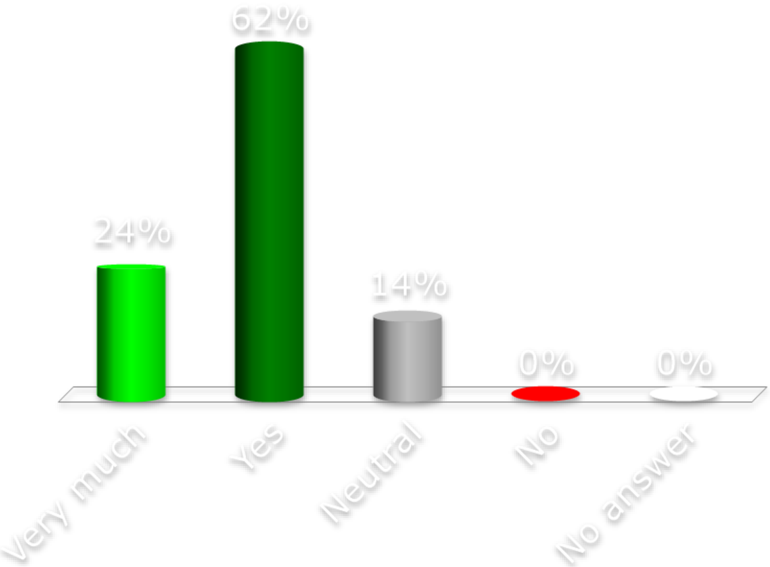
Question 1: Did you like this exercise?

A. Very much
B. Yes
C. Neutral
D. No
E. No answer



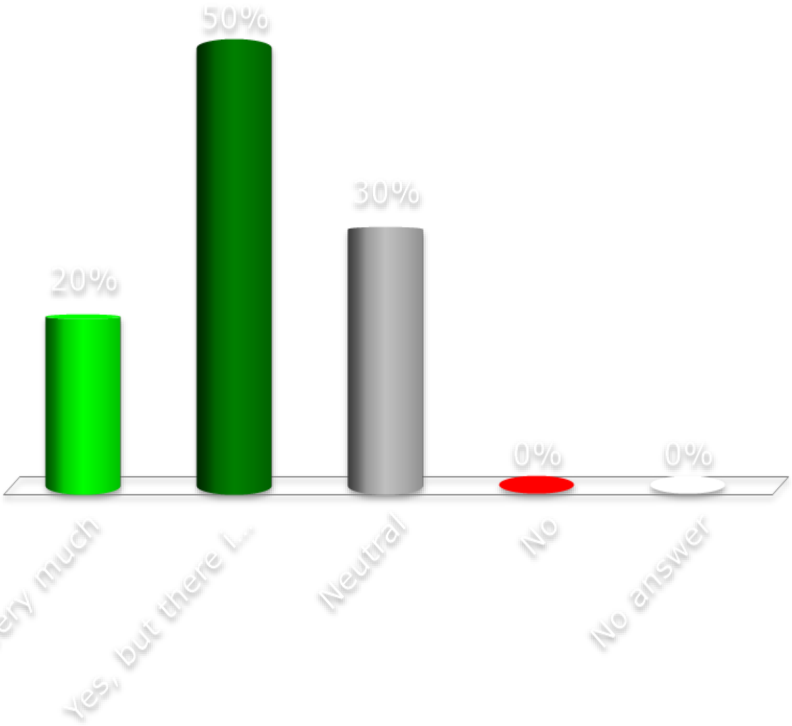
Question 2: Did you find the scenario relevant?

A. Very much
B. Yes
C. Neutral
D. No
E. No answer



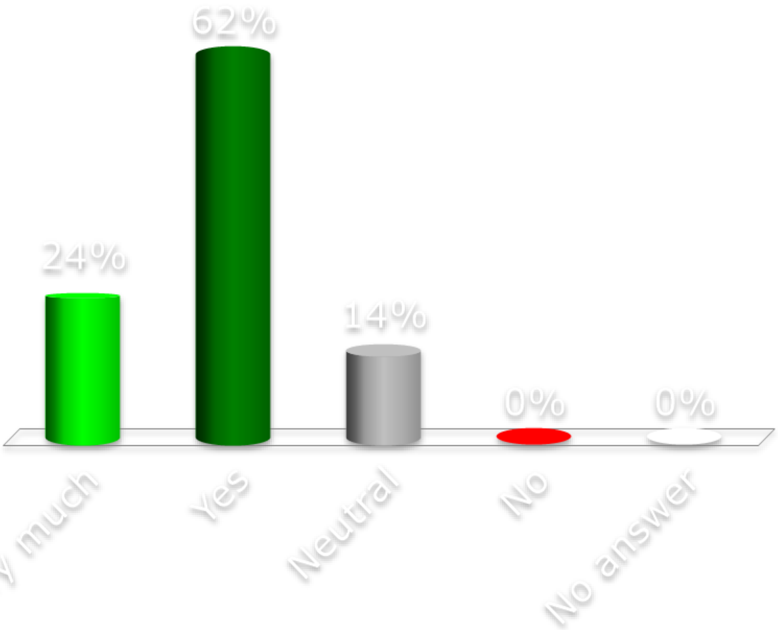
Question 3: Did you like the organization of this exercise?

A. Very much
B. Yes, but there is room for improvement
C. Neutral
D. No
E. No answer



Question 4: Did EUELEx19 add value to your efforts for safer EU elections?

A. Yes
B. Partially yes
C. Neutral
D. No
E. No answer



XX-00-00-000-XX-X

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 Europe’s citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000