



---

# Advancing Regional Cybersecurity (ARC) KENYA

## Tabletop exercise annex

4 May 2026

Authors: Elizabeth Eigner, Patricia Eke, Colonel (Dr) James Kimuyu, PhD, Markus Münzer

# ANNEX 1

## Exercise Content & Results

The following section presents the exercise content and results inject by inject, with the following structure:

- Inject Title
- Inject Body & Answer Options (if applicable)
- Full Aggregate Statistics in Working Groups for Joint Injects
  - All
  - WG1: Cybersecurity Governance
  - WG2: General Governance
  - WG3: Private Sector & Industry
  - WG4: Civil Society & Academia
- Group-Based Aggregate Statistics for Group-Specific Injects
- Open-Ended Responses & Comments

### Inject 0.1 – PREVIOUS INCIDENTS AND CRISES

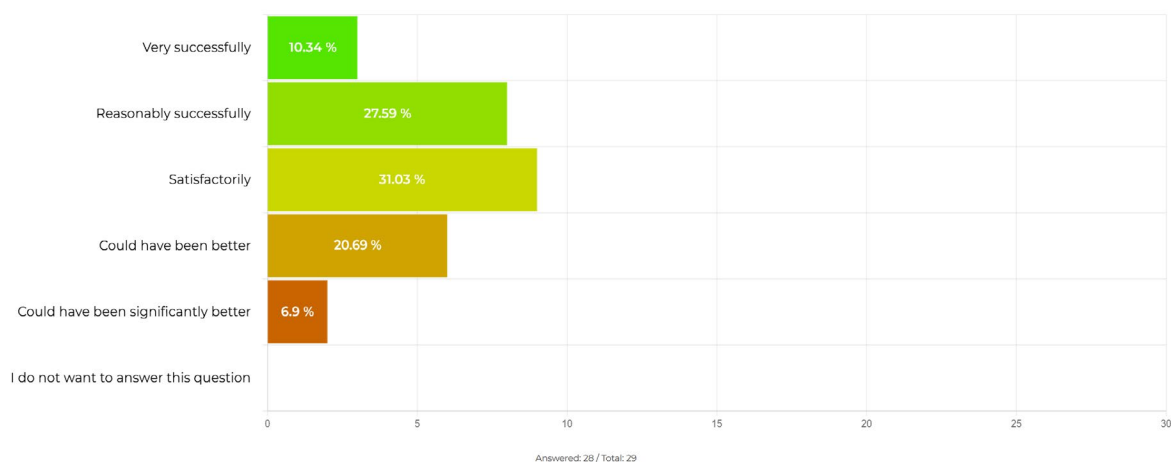
In your opinion, how has your nation dealt with recent cyber incidents and crises?

- Very successfully
- Reasonably successfully
- Satisfactorily
- Could have been better
- Could have been significantly better
- I do not want to answer this question

All

## 0.1 - PREVIOUS INCIDENTS AND CRISES

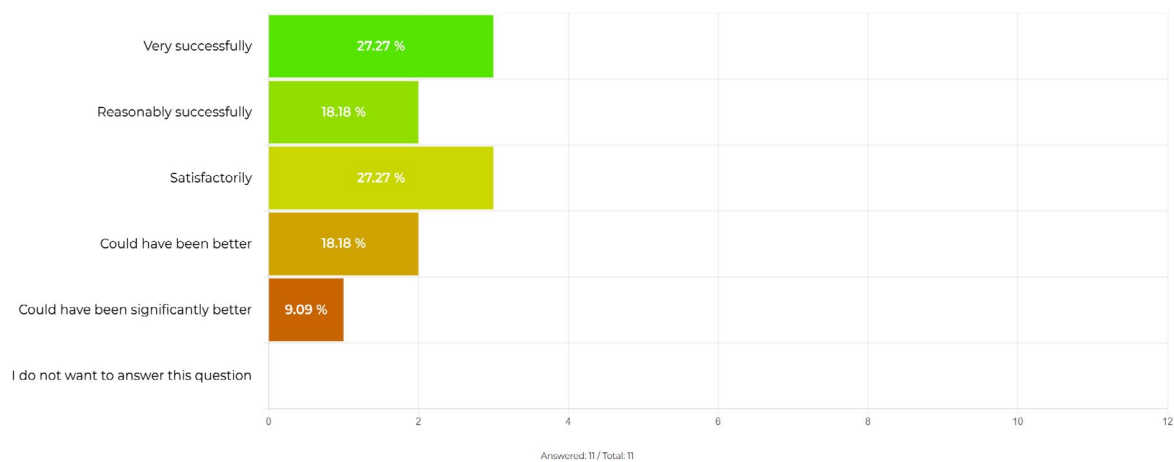
In your opinion, how has your nation dealt with recent cyber incidents and crises?



WGT: Cybersecurity Governance

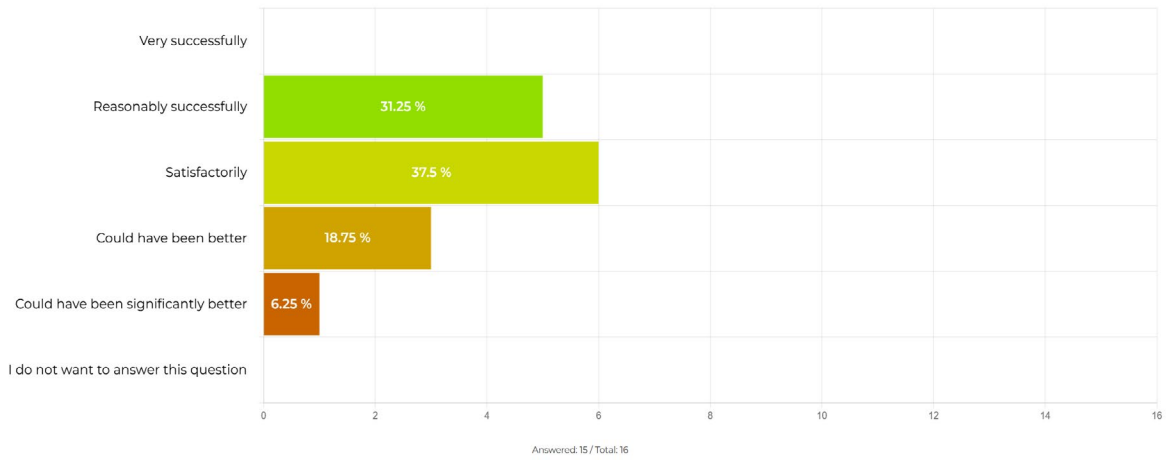
## 0.1 - PREVIOUS INCIDENTS AND CRISES

In your opinion, how has your nation dealt with recent cyber incidents and crises?



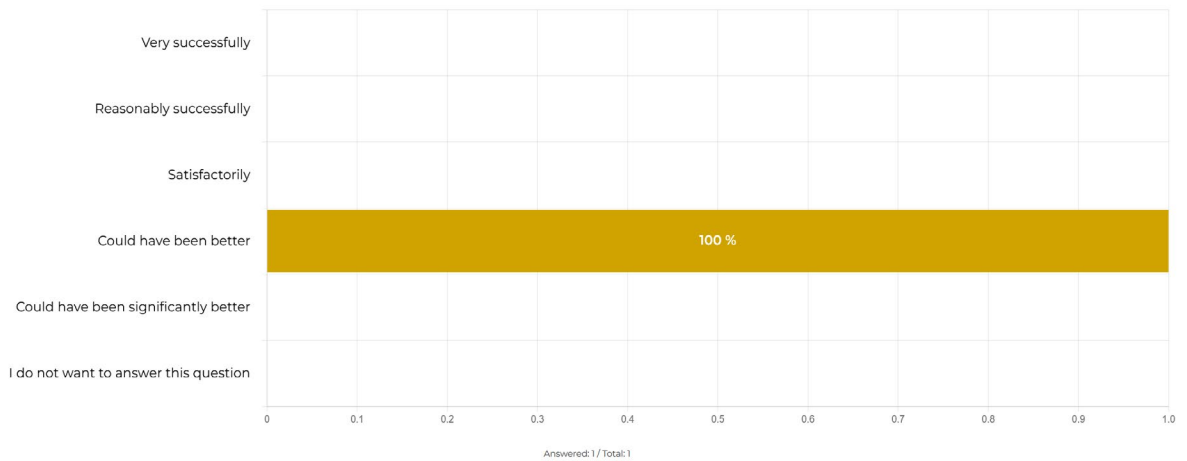
## 0.1 - PREVIOUS INCIDENTS AND CRISES

In your opinion, how has your nation dealt with recent cyber incidents and crises?



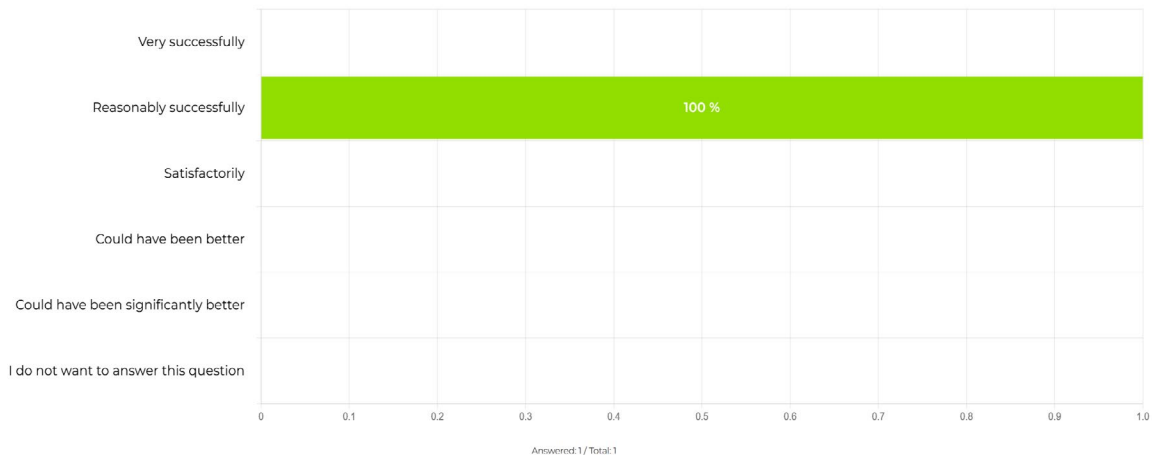
## 0.1 - PREVIOUS INCIDENTS AND CRISES

In your opinion, how has your nation dealt with recent cyber incidents and crises?



## 0.1 - PREVIOUS INCIDENTS AND CRISES

In your opinion, how has your nation dealt with recent cyber incidents and crises?



## Comments:

- Better frameworks and strategies (**Gen Gov09**) (**Could have been better**)
- It was awesome. It opened my eyes to a lot of things I did not know I knew (**Cyb Gov08**) (**Very successfully**)
- There is always room to improve based on lessons learned (**Gen Gov14**) (**Could have been significantly better**)
- Duration of response was a bit long (**Gen Gov10**) (**Satisfactorily**)
- Avoid zero-day vulnerability by timely patching (**Gen Gov08**) (**Reasonably successfully**)
- The designated state department is able to address the issues within a short time (**Gen Gov13**) (**Satisfactorily**)
- Significant improvements need to be made in capacity building, policy enforcements and procurement of tools. (**Cyb Gov07**) (**Could have been better**)
- The services were restored in a short time frame (**Gen Gov12**) (**Reasonably successfully**)
- Misinformation took the better part before incidence response (**Gen Gov11**) (**Satisfactorily**)
- Did the most with what they had (**Cyb Gov11**) (**Satisfactorily**)
- Remediation and cause of attack not shared to other sectors/ mcdas (**Gen Gov15**) (**Satisfactorily**)
- Improve on infrastructure and capacity build staff (**Cyb Gov10**) (**Could have been better**)
- The recovery time was commendable (**Cyb Gov09**) (**Reasonably successfully**)
- The restoration of services after recent cyberattacks have taken a bit of time and coordination from several stakeholders. (**Academia01**) (**Reasonably successfully**)

## Inject 0.2 – CHALLENGES IN DEALING WITH CYBER THREATS

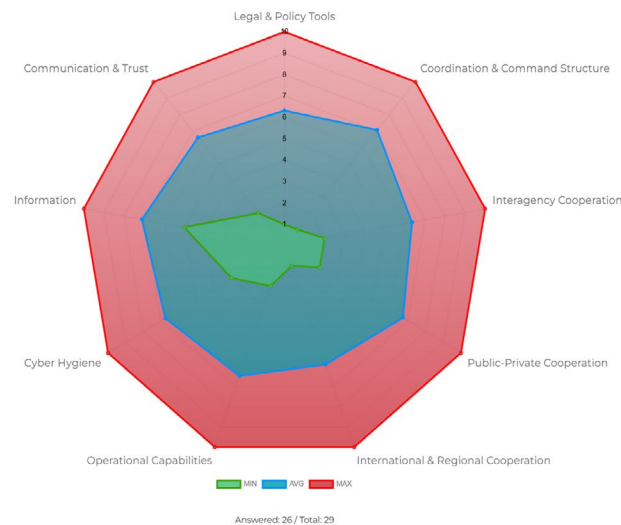
On the scale of 1 – 10, where 10 is the most significant and 1 is the least significant, please assess some of the greatest challenges in formulating effective response to cyber threats. You can assign the same number for multiple times and you do not need to use all numbers.

- Legal and policy tools for cyber response
- National coordination and command structure
- Interagency cooperation in practice
- Public-private cooperation
- International and regional cooperation
- Operational cyber detection and response capabilities
- Inadequate levels of cyber hygiene
- Attribution, intelligence and situational awareness
- Crisis communication and public trust management

All

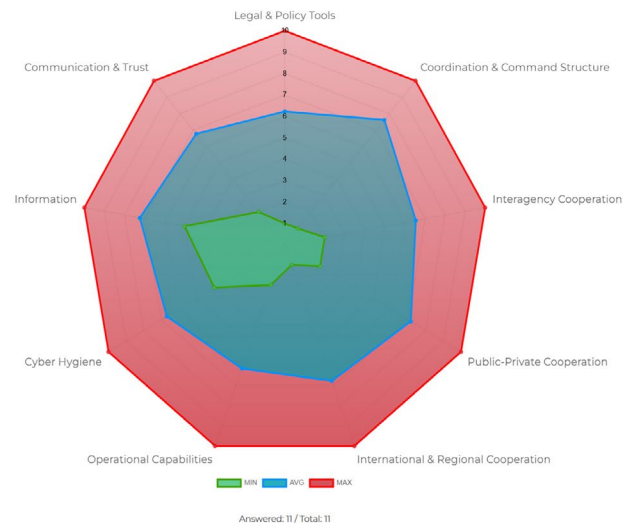
### 0.2 - CHALLENGES IN DEALING WITH CYBER THREATS

On the scale of 1 – 10, where 10 is the most significant and 1 is the least significant, please assess some of the greatest challenges in formulating effective response to cyber threats. You can assign the same number for multiple times and you do not need to use all numbers.



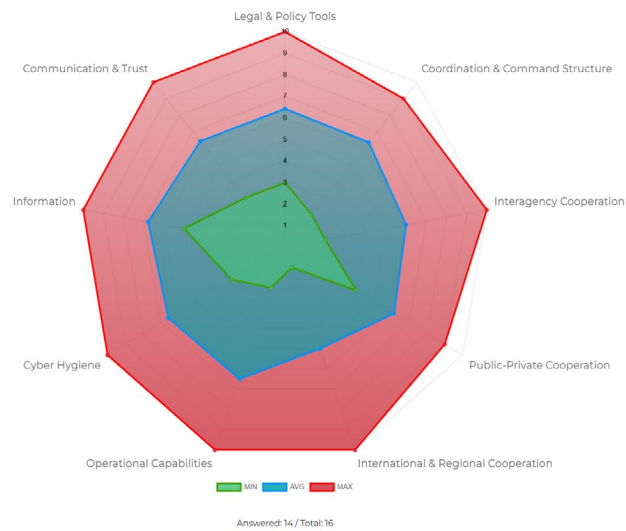
## 0.2 - CHALLENGES IN DEALING WITH CYBER THREATS

On the scale of 1 – 10, where 10 is the most significant and 1 is the least significant, please assess some of the greatest challenges in formulating effective response to cyber threats. You can assign the same number for multiple times and you do not need to use all numbers.



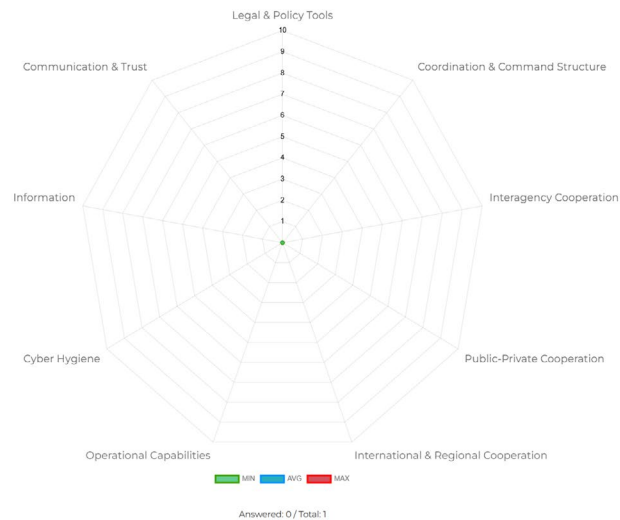
## 0.2 - CHALLENGES IN DEALING WITH CYBER THREATS

On the scale of 1 – 10, where 10 is the most significant and 1 is the least significant, please assess some of the greatest challenges in formulating effective response to cyber threats. You can assign the same number for multiple times and you do not need to use all numbers.



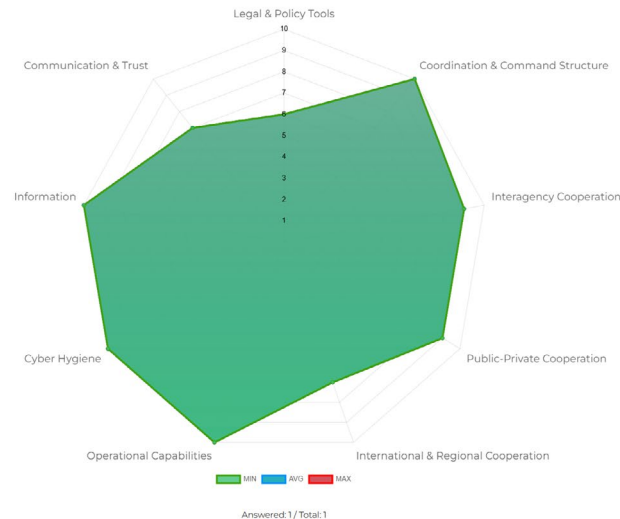
## 0.2 - CHALLENGES IN DEALING WITH CYBER THREATS

On the scale of 1 – 10, where 10 is the most significant and 1 is the least significant, please assess some of the greatest challenges in formulating effective response to cyber threats. You can assign the same number for multiple times and you do not need to use all numbers.



## 0.2 - CHALLENGES IN DEALING WITH CYBER THREATS

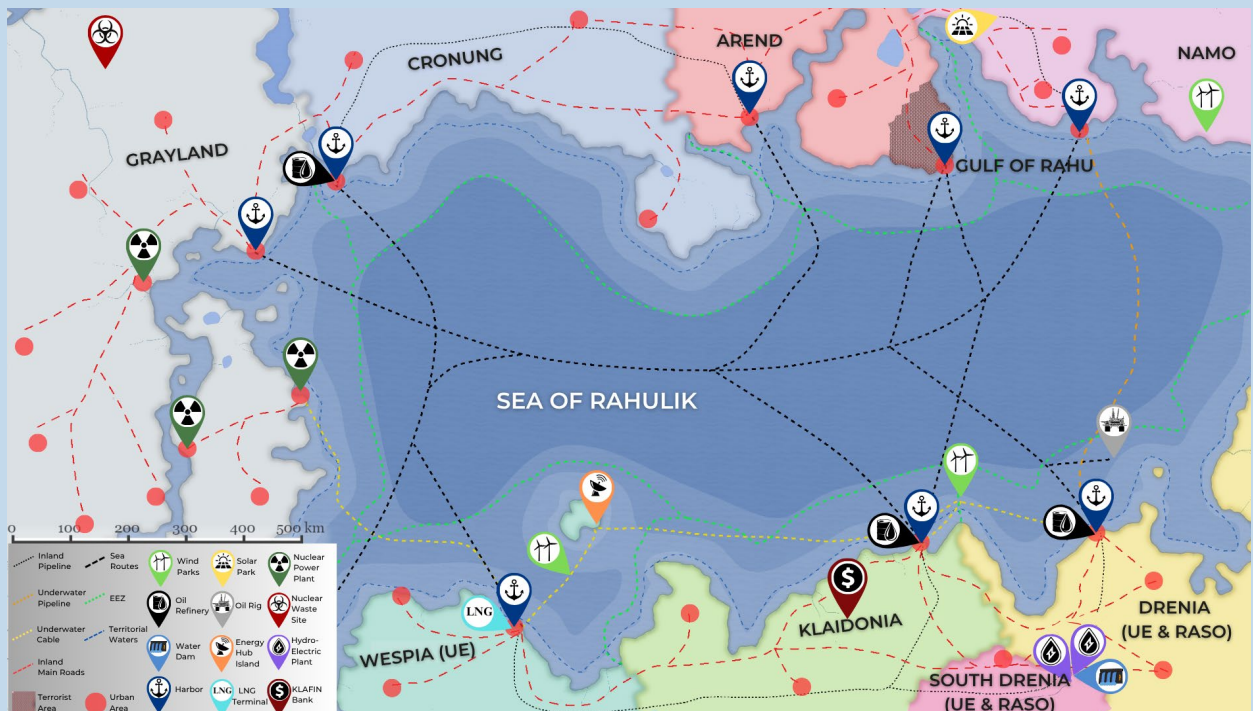
On the scale of 1 – 10, where 10 is the most significant and 1 is the least significant, please assess some of the greatest challenges in formulating effective response to cyber threats. You can assign the same number for multiple times and you do not need to use all numbers.



## Comments:

- I believe there is still some great room for improvement (Cyb Gov08)

## Inject 0.3 – THE LEGEND



### Comments:

**CRONUNG.** A former regional powerhouse with vast oil and gas reserves. Once a federal state, CRONUNG is now fragmented, with rival governments, militias, and external actors competing for control. Several regions sit atop significant energy deposits, while others are attempting to attract foreign investment in renewable energy. CRONUNG has repeatedly interfered in neighbouring states, supporting proxy groups and using hybrid tactics to project influence across the region.

**WESPIA.** A maritime state controlling access between the Rahulik Sea. Its economy is built on shipping and port services, hosting several international logistics and shipping companies. WESPIA has recently expanded into the LNG market, establishing an offshore terminal that supplies gas to neighbouring countries.

**KLAIDONIA.** A like-minded RASO nation without major domestic fossil fuel resources. KLAIDONIA's national energy company, KLADOIL, manages the largest oil refinery in the region. The KLAIDONIAN state owns a significant share of the refinery, which plays a strategic role in regional energy security. KLADOIL is also a leading investor in renewable energy projects,

especially in NAMO, where it is financing large solar and wind parks. Furthermore, KLAFIN, one of the largest retail and wholesale banks in the region resides in the country, serving also WESPIA and DRENIA.

**DRENIA.** A RASO partner with substantial offshore gas fields in its Exclusive Economic Zone. DRENIA has benefited from shifts in global energy flows, as states that once relied on CRONUNG's oil and gas now import from DRENIA. At the same time, it has committed to the UE's green energy transition policies. DRENIA's new wealth makes it a key player in the Rahulik region.

**SOUTH-DRENIA.** A RASO partner historically linked to DRENIA. SOUTH-DRENIA benefits economically from being a transit state for regional pipelines. It also has untapped hydropower potential. Recently, SOUTH-DRENIA has held negotiations with its wealthier neighbour DRENIA over the future of shared pipeline infrastructure and revenue-sharing.

**NAMO.** A cooperative state seeking stronger alignment with the democratic community. For decades, NAMO has been vulnerable to CRONUNG's influence. With vast uninhabited lands suitable for energy projects, NAMO has become a hub for international solar and wind energy investment. It also serves as a critical transit corridor for a gas pipeline carrying natural gas to coastal export terminals.

**AREND.** A fragile democratic-leaning state under heavy pressure from CRONUNG. In one region, the separatist movement DEMOCRATIC AREND (DEAR) operates with direct support from CRONUNG. DEAR has carried out hybrid and cyberattacks across the Rahulik Sea region in recent years, destabilising neighbouring countries and maritime routes.

**GRAYLAND.** A neutral country that historically acted as a buffer between CRONUNG and democratic nations. GRAYLAND has reduced its dependence on CRONUNG's oil and gas, shifting instead toward renewable energy with UE support. It now plays an increasingly important role in regional security and maritime stability.

**UNION OF ECONOMY (UE).** A supranational political and economic union supporting democracy, resilience, and green transition in Africa. The UE is a major partner for both KLADONIA and NAMO, providing investment in renewables, security cooperation, and political support.

**RAHULIK AREA SECURITY ORGANIZATION (RASO).** A regional political and military alliance supporting collective defence and crisis management. KLADONIA is an active RASO member, seeking deeper engagement in cybersecurity and maritime security initiatives.

## Inject 0.4 – AFFILIATIONS & POSTURE

| COUNTRY      | UE   | RASO | POSTURE  |
|--------------|------|------|----------|
| CRONUNG      | NO   | NO   | HOSTILE  |
| AREND        | NO   | NO   | HOSTILE  |
| NAMO         | NO   | NO   | NEUTRAL  |
| WESPIA       | YES  | NO   | FRIENDLY |
| DRENIA       | YES  | YES  | FRIENDLY |
| SOUTH-DRENIA | YES  | YES  | FRIENDLY |
| GRAYLAND     | NO   | NO   | NEUTRAL  |
| KLAIDONIA    | HOME | HOME | HOME     |

## Inject 0.5 – SCENE SETTING

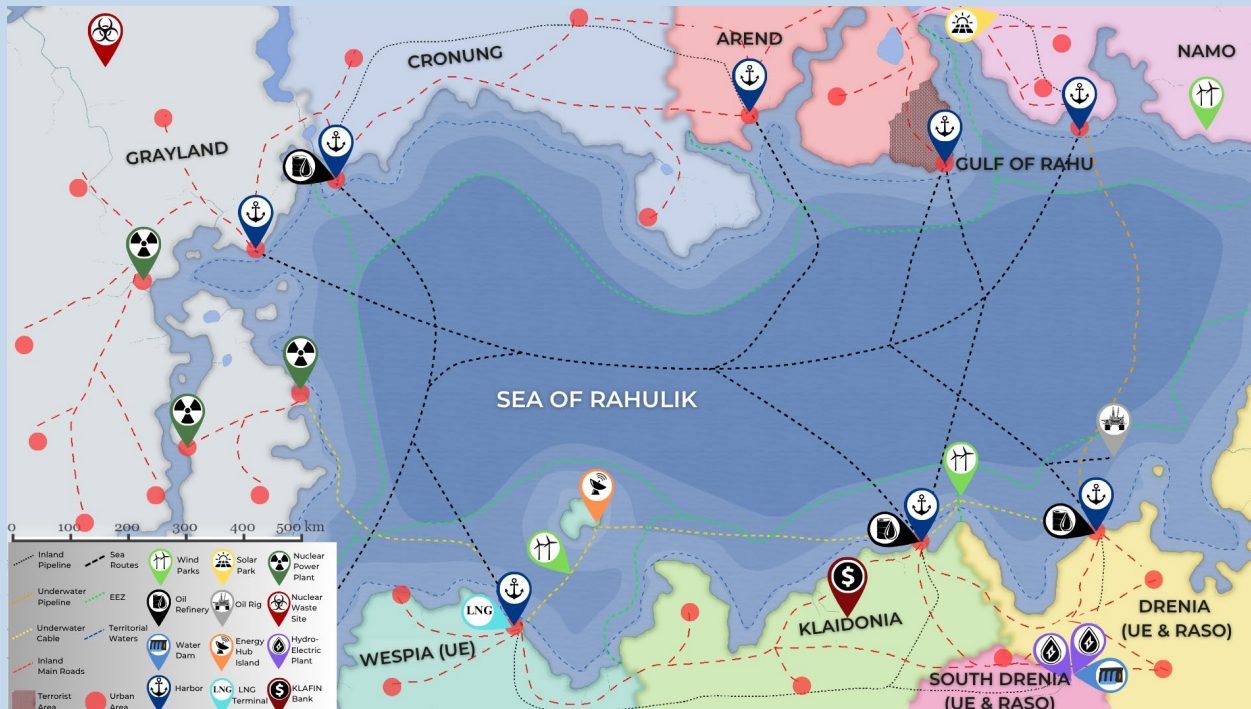
**RAHULIK SEA** region is a place where various competing interests, driven by different values and race for resources and energy independence collide. In the North, the area is dominated by often aggressive and authoritarian CRONUNG. The country is controlled by a small group of people who derive their authority from the command of various intelligence agencies and military structures. The country's economy has suffered due to severe mismanagement, corruption, and failure of market reforms.

**CRONUNG** shares a border with AREND – a democratic leaning country, with fragile government, immature rule of law and rising economy. The country faces a considerable challenge in the southern part of its territory. AREND is dependent on the energy resources on CRONUNG and is dependent on its support in solving the crisis in SOUTH AREND PENINSULA. The peninsula is currently controlled by para-military group DEMOCRATIC AREND (DEAR) that UE countries have

designated as a terrorist organization. They occupy a geographically significant area that can affect sea routes, in the GULF OF RAHU, underwater cables and critical port of NEW AREND. The conflict benefits CRONUNG as it drives the AREND government to a greater dependency from their resources and it gives its special services an ability to secretly collaborate with DEAR units. The disputed area is uncomfortably close to NAMO, who has carried out successful market and governance reforms and is building close economic cooperation with UE countries. One of the most important goals of the cooperation for NAMO is to build a solid energy independence from CRONUNG whom they still rely on some energy supply. This has prompted the Government of NAMO to invest in renewable energy production like wind farms and solar parks. Often, they use international energy companies to construct the sites. NAMO has a good relationship with KLAIDONIA and DRENIA, whose companies have often been successful in winning contracts to develop the sites.

On the Southern flank of RAHULIK SEA situates four democratic countries which are members of UE; GRAYLAND, WESPIA, DRENIA and SOUTH-DRENIA. All those countries, however, also face challenges including in Energy Security. KLAIDONIA and DRENIA are working closely with NAMO to create greater energy independence in the region through investing in renewable energy production. This includes supporting considerable investments in NAMO by their energy companies. DRENIA is very strongly committed in renewable energy production. In the recent elections a party promising to increase renewable energy production by 75% in the coming years won the majority of the votes. At the same time, SOUTH DRENIA relies on the oil pipeline that passes through DRENIA. With recent political changes in DRENIA, the fate of the oil pipeline has become under question and is causing tensions between DRENIA and SOUTH DRENIA that is also exploited by CRONUNG.

## Inject 1.1 – CYBERSECURITY GOVERNANCE & GENERAL GOVERNANCE: SITUATION REPORT



### Comments:

KLADOIL and KLAIDONIA Ministry of Energy is sharing information, that the power outage has been accompanied by numerous distributed denial of service (DDoS) attacks on several Critical Energy Infrastructure organizations, responsible for the maintenance and management of power grids as well as distribution on electricity

In addition, such DDoS attacks are also reported by WESPIAN authorities. Targets of the attackers are primarily public services that provide end-user level interaction including managing of contracts, emergency alerts regarding power consumption thresholds, outage notices etc.

The WESPIAN CERT has reported comprehensive scanning of networks.

Some of the IP-addresses used in the attacks are originating from AREND, whilst the majority of them currently remain unattributable.

## **Inject 1.1 – PRIVATE SECTOR & INDUSTRY: SITUATION REPORT**

KLADOIL is experiencing numerous distributed denial of service (DDoS) attacks on several energy instalments, responsible for the maintenance and management of power grids as well as distribution on electricity.

Seemingly, end-user level public services responsible for managing of contracts, emergency alerts regarding power consumption thresholds, outage notices are disrupted.

At this stage, there has been no contact made by any adversary.

## **Inject 1.1 – CIVIL SOCIETY & ACADEMIA: SITUATION REPORT**

The KLADOIL energy management software suite appears to be disrupted with significant delays or even outages in their applications.

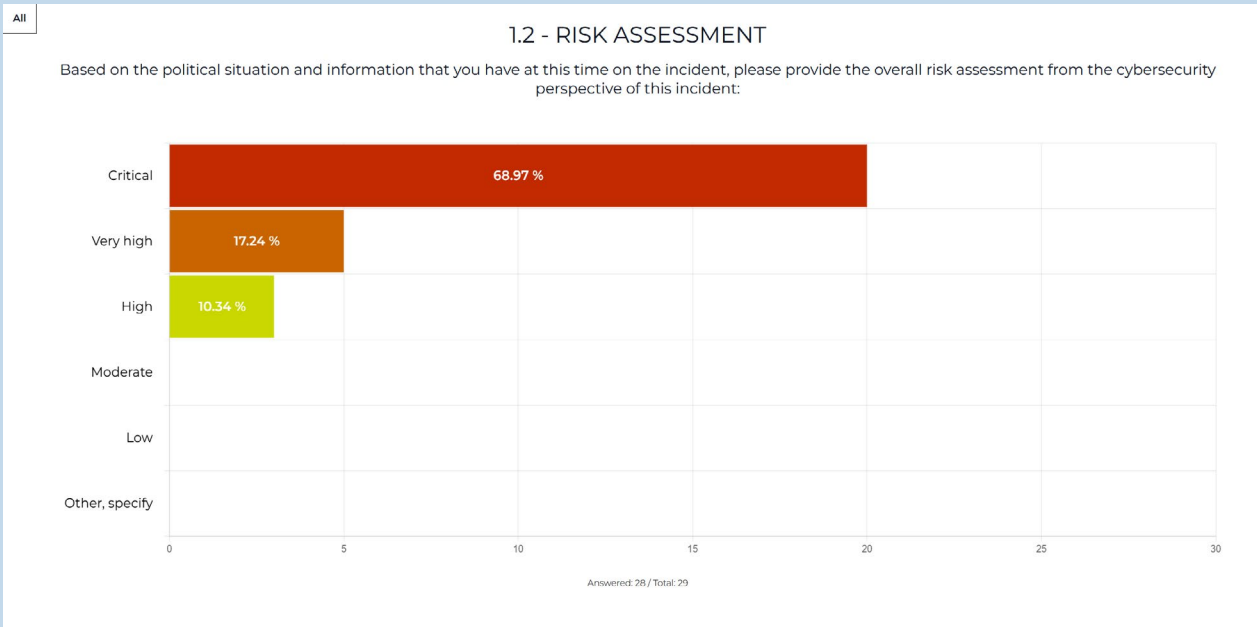
Seemingly, services responsible for managing of contracts, emergency alerts regarding power consumption thresholds, outage notices are disrupted.

At this stage, there is no notification from KLADOIL on this incident.

Inject 1.2 – RISK ASSESSMENT

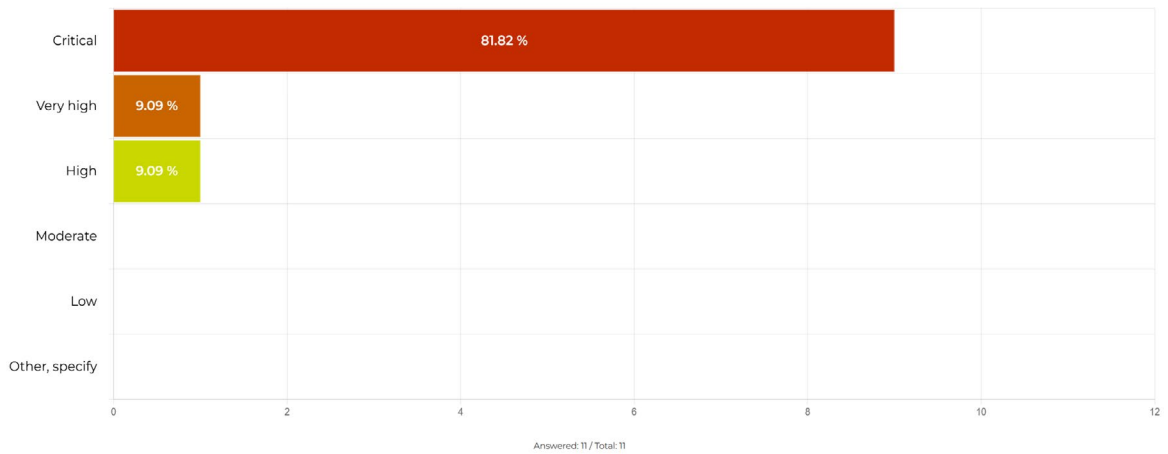
Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:

- Critical
- Very high
- High
- Moderate
- Low
- Other, specify \_\_\_\_\_



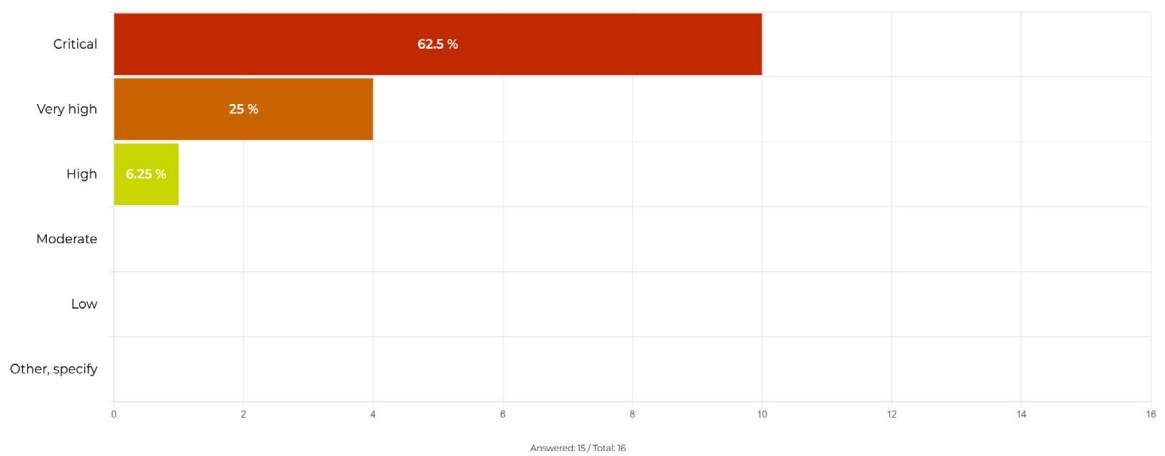
## 1.2 - RISK ASSESSMENT

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



## 1.2 - RISK ASSESSMENT

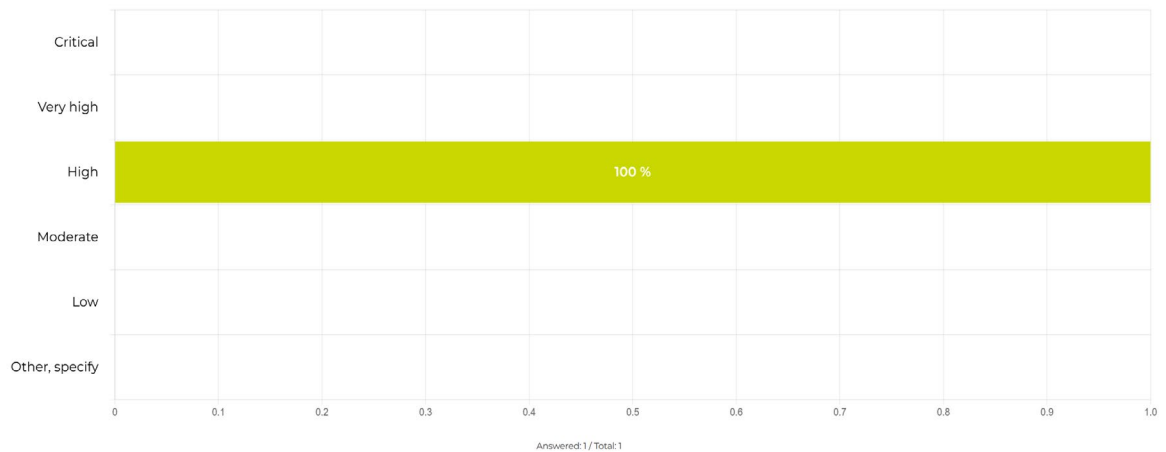
Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



WG3: Private Sector

## 1.2 - RISK ASSESSMENT

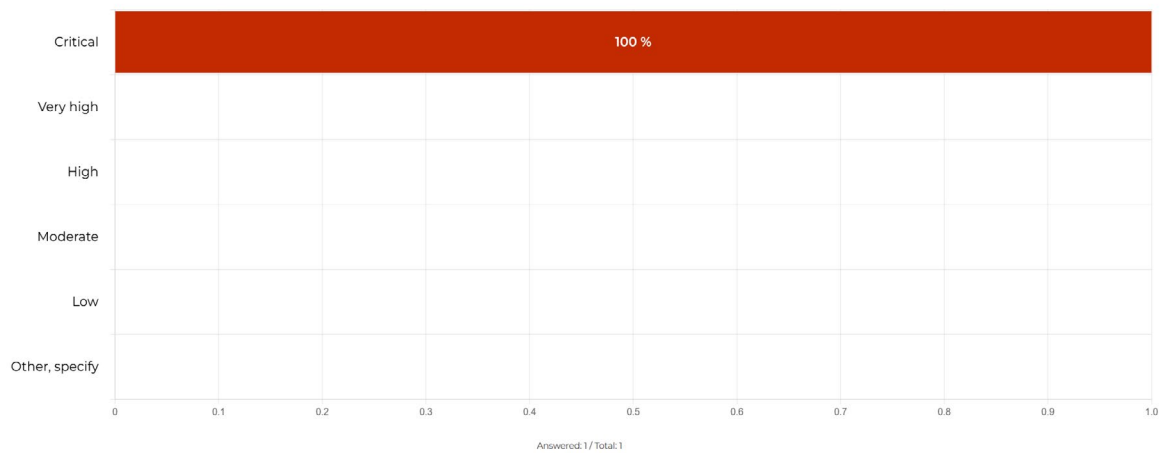
Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



WG4: Academia

## 1.2 - RISK ASSESSMENT

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



## Comments:

- Because it has impact on the National Critical Infrastructure which could be disastrous to the whole country **(Gen Gov13) (Critical)**
- This is critical because many countries are being affected at the same time. The anonymity of the group that causes this is also a major concern that poses a high risk. **(Cyb Gov10) (Critical)**
- The threat is on infrastructure, and the affected nation has classified it as an act of war. This can easily escalate to a full-blown war. **(Cyb Gov09) (Critical)**
- Critical Energy infrastructure has been affected, target is Government Agencies offering end user services. Disruption of power greatly impacts many other operations that could potentially lead to greater risks **(Cyb Gov04) (Critical)**
- The DDOS attack cuts across sectors and countries. Not only are public services inaccessible in Wespia including shipping, Kladoil clients are experiencing service disruptions which affects nation economic ties and trade which will cause a domino effect on other sectors. **(Cyb Gov07) (Critical)**
- Critical infrastructure has also been affected making it very critical **(Cyb Gov10) (Critical)**
- This is a critical infrastructure that will end up affecting the region as well as the economy of the country **(Cyb Gov08) (Critical)**
- The power outage, the cable cut and the disruption of services aggregate to negatively impact energy security and national security. The economic security is also affected. **(Academia01) (Critical)**
- IP address reporting blocking critical services are not accessed by users due to denial of service **(Gen Gov09) (Did not answer)**
- Risk = likelihood x impact. Therefore, the product of high (5) and impact (5) gives Critical (25). Based on a scale of 1-5. **(Cyb Gov02) (Critical)**

## Inject 1.3 – SEVERITY OF THE SITUATION

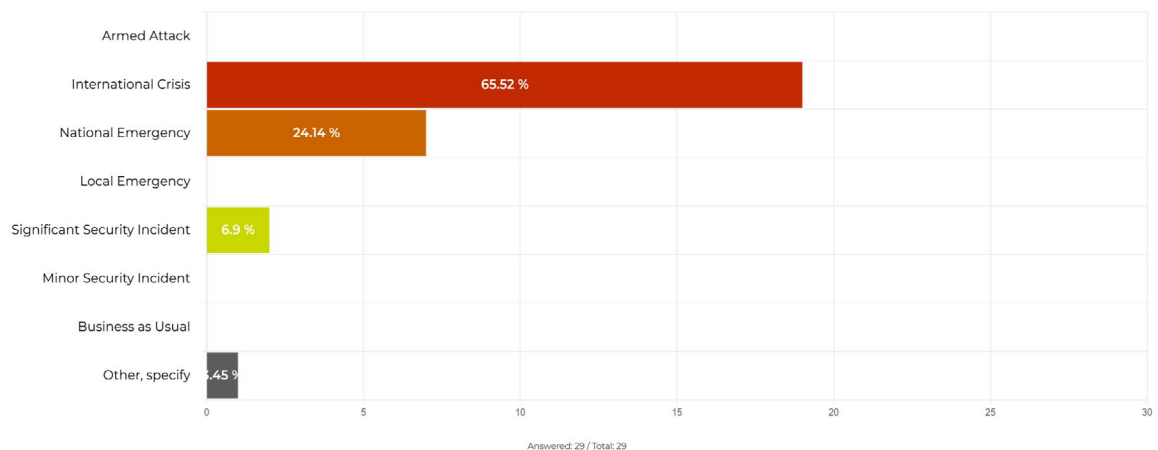
Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:

- Armed Attack
- International Crisis
- National Emergency
- Local Emergency
- Significant Security Incident
- Minor Security Incident
- Business as usual
- Other, specify: \_\_\_\_\_

All

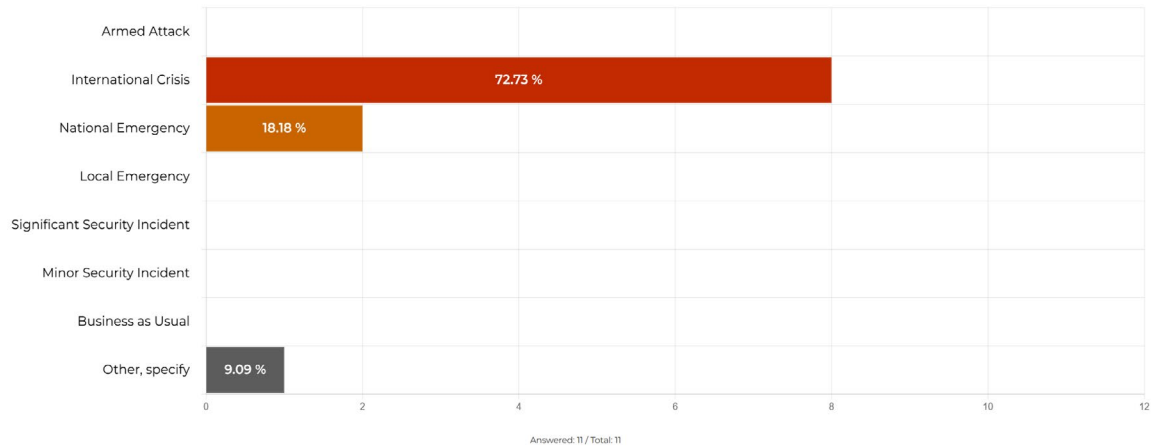
### 1.3 - SEVERITY OF THE SITUATION

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



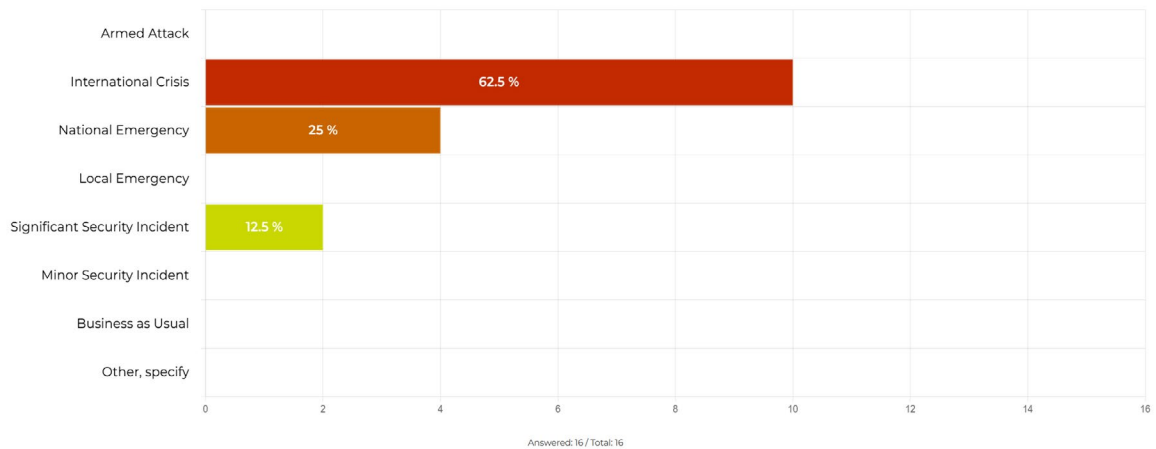
## 1.3 - SEVERITY OF THE SITUATION

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



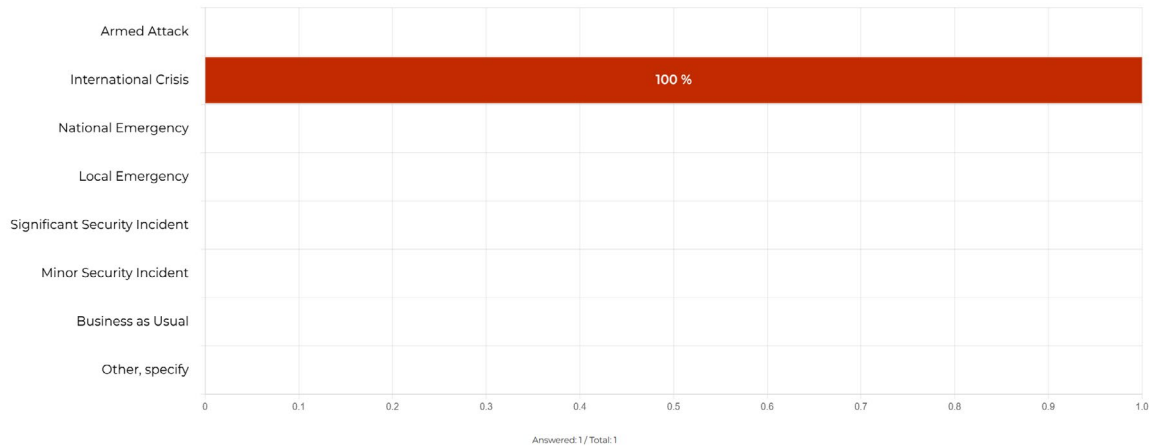
## 1.3 - SEVERITY OF THE SITUATION

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



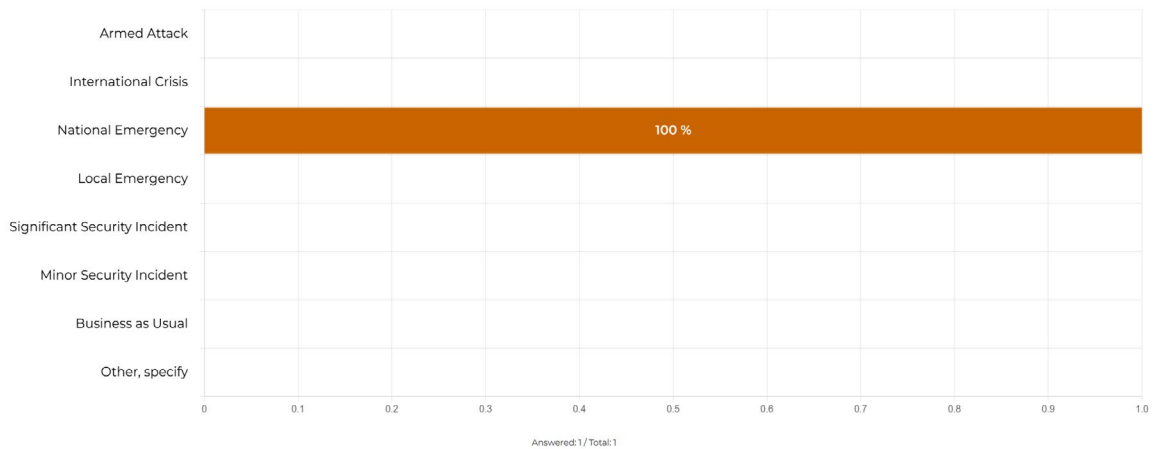
## 1.3 - SEVERITY OF THE SITUATION

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



## 1.3 - SEVERITY OF THE SITUATION

Based on the political situation and information that you have at this time on the incident, please provide the overall risk assessment from the cybersecurity perspective of this incident:



### Other, specify:

- It is both an international crisis and a national emergency for Wespia (Cyb Gov07)

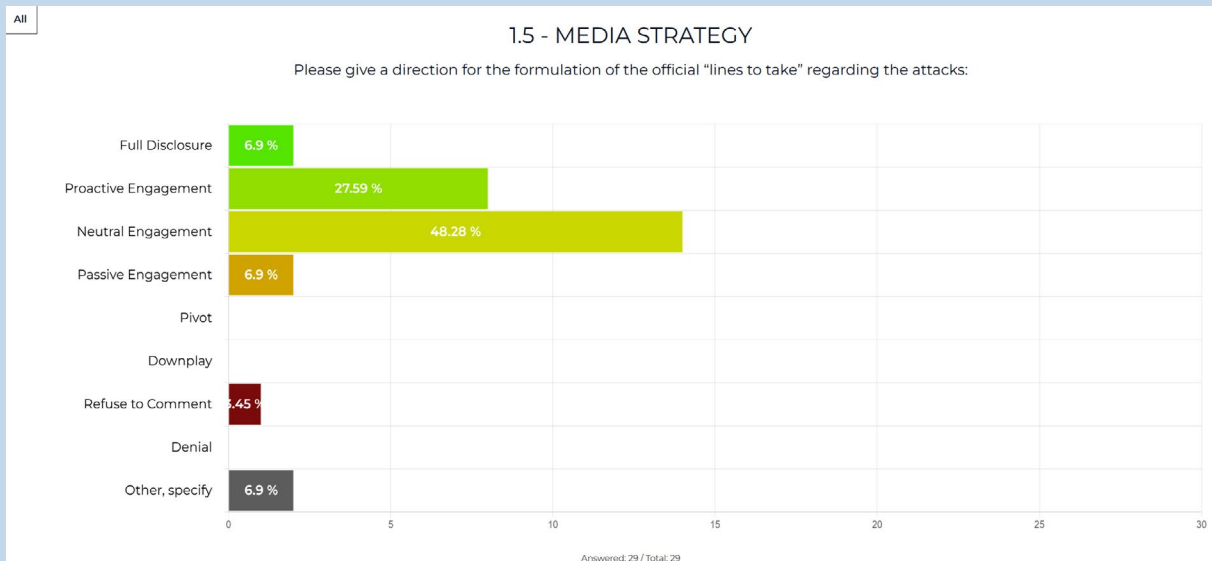
## Comments:

- Attribution seems to go beyond our borders (**Gen Gov01**) (**National Emergency**)
- Could spark a diplomatic wrangle (**Gen Gov2**) (**Significant Security Incident**)
- Affects many countries (**Cyb Gov10**) (**International Crisis**)
- The region will be highly affected (**Cyb Gov08**) (**International Crisis**)
- Risk of DDoS ,power interruption and IP address coming from affiliate of bad actor (**Gen Gov08**) (**Significant Security Incident**)
- Since Its affecting critical infrastructure-OT, might move across (**Academia01**) (**National Emergency**)
- Political instability (**Gen Gov09**) (**National Emergency**)
- Because the infrastructure affected several countries. (**Cyb Gov09**) (**International Crisis**)
- Policy risks (**Gen Gov09**) (**National Emergency**)
- The situation is likely to cascade across the entire country. Besides, as a country, you concentrate first on national interest. (**Academia01**) (**National Emergency**)

## Inject 1.5 – MEDIA STRATEGY

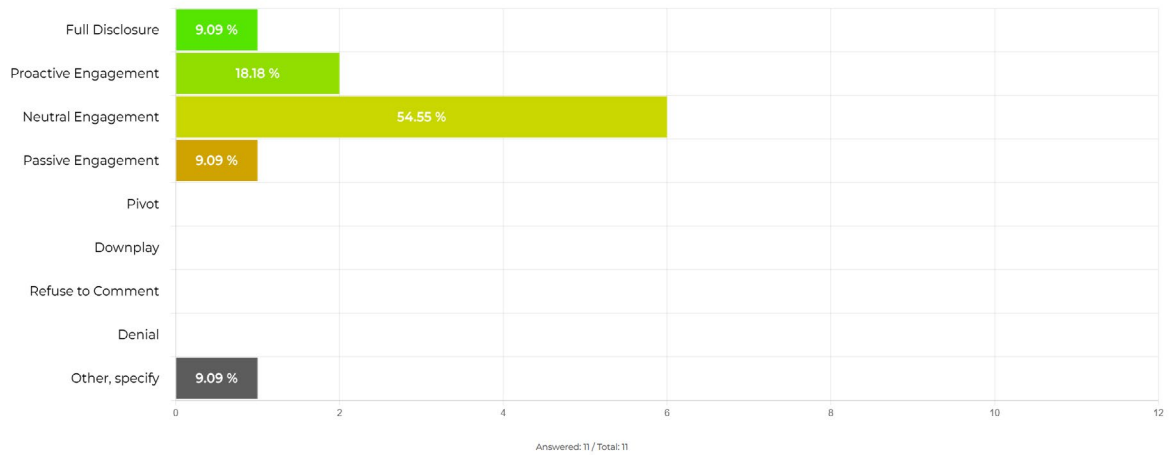
Please give a direction for the formulation of the official “lines to take” regarding the attacks:

- Full Disclosure: Provide full disclosure to authorities, customers and the public
- Proactive Engagement: Explain the situation, provide deep background briefings to the media
- Neutral Engagement: Confirm the situation and share minimum amount of facts
- Passive Engagement: Confirm the situation only if asked
- Pivot: Divert media attention to other topics
- Downplay: Describe the situation as routine technical glitch not worthy of attention
- Refuse to Comment: Refuse to comment for security, investigative or other national/legal reasons
- Denial: Deny the situation altogether
- Other, specify: \_\_\_\_\_



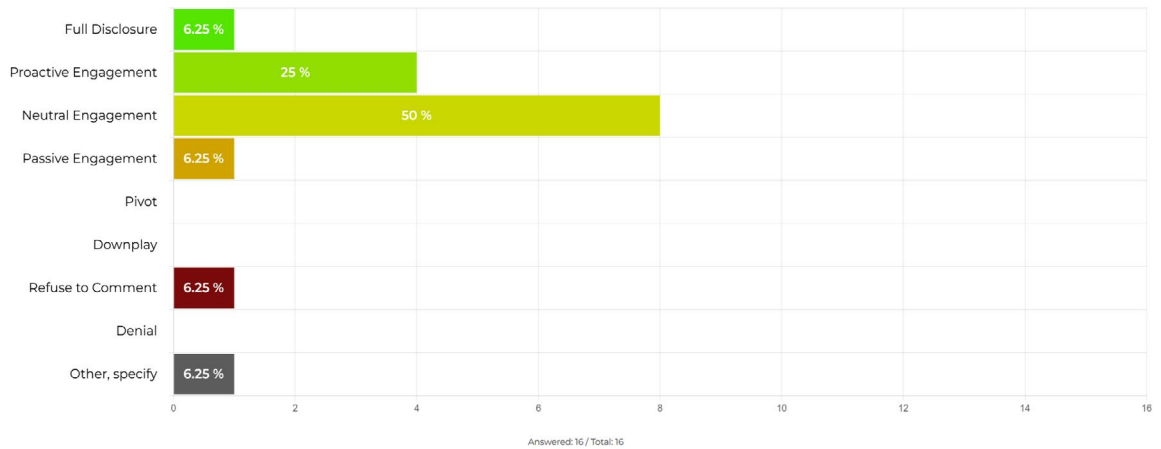
## 1.5 - MEDIA STRATEGY

Please give a direction for the formulation of the official "lines to take" regarding the attacks:



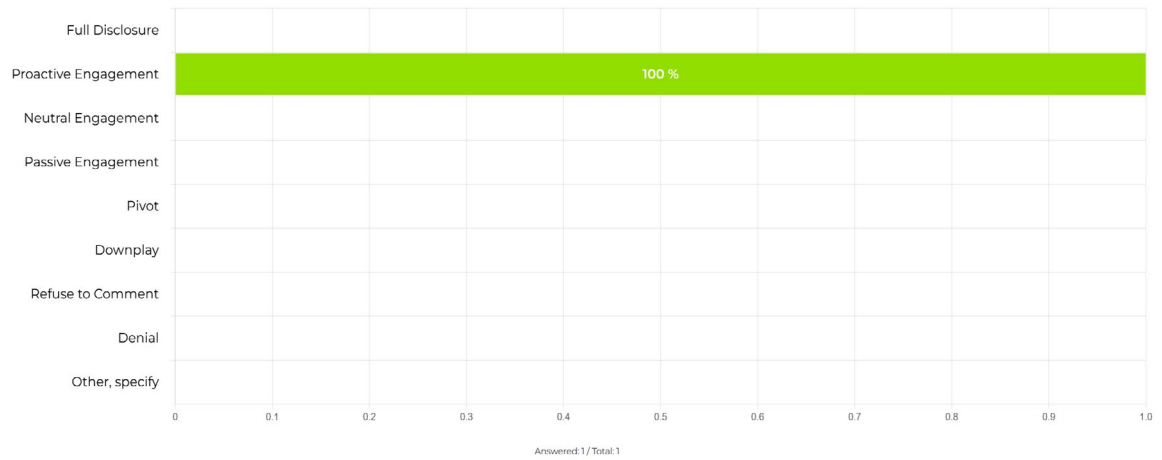
## 1.5 - MEDIA STRATEGY

Please give a direction for the formulation of the official "lines to take" regarding the attacks:



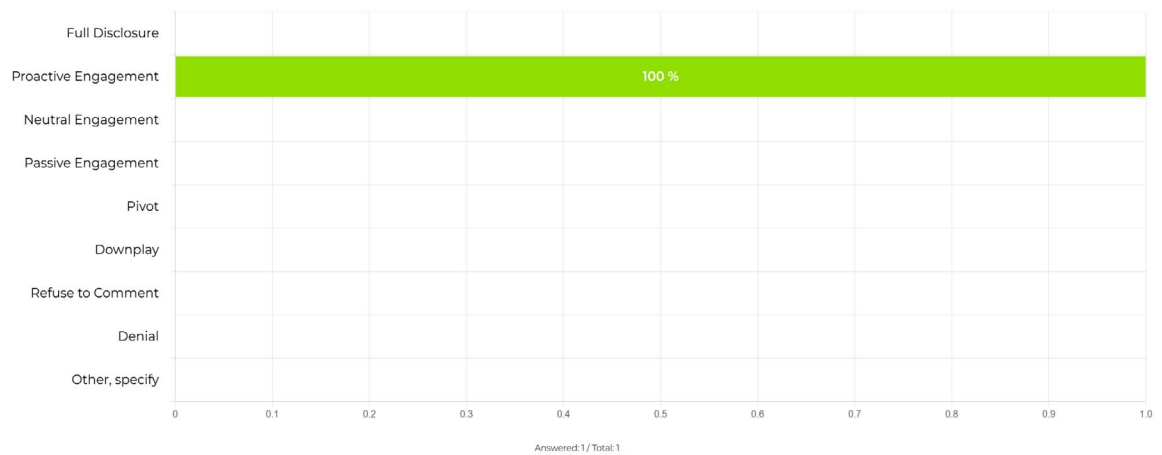
## 1.5 - MEDIA STRATEGY

Please give a direction for the formulation of the official "lines to take" regarding the attacks:



## 1.5 - MEDIA STRATEGY

Please give a direction for the formulation of the official "lines to take" regarding the attacks:



### **Other, specify:**

- Provide full disclosure to relevant authorities and important stakeholders and only relevant information to the public **(Cyb Gov04)**
- Confirm to the public and stakeholders the incident occurred and that you will give more details once the investigations are done **(Gen Gov2)**

### **Comments:**

- Full disclosure may likely cause national apprehension. **(Academia01) (Proactive Engagement)**
- The less the better **(Gen Gov14) (Neutral Engagement)**
- Consider key aspects of a foreign policy such as deescalating tension between states and avoiding provocative actions within the cyberspace. **(Cyb Gov02) (Proactive Engagement)**

## Inject 1.6 – ACCEPTABLE SERVICE DOWNTIME

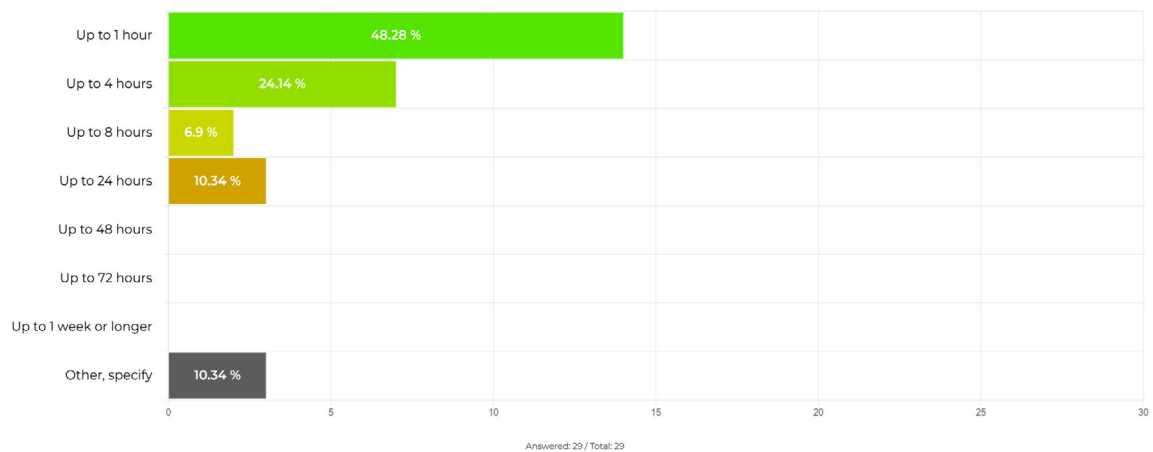
What would be the acceptable service downtime for national critical energy infrastructure?

- Up to 1 hour
- Up to 4 hours
- Up to 8 hours
- Up to 24 hours
- Up to 48 hours
- Up to 72 hours
- Up to 1 week or longer
- Other, specify \_\_\_\_\_

All

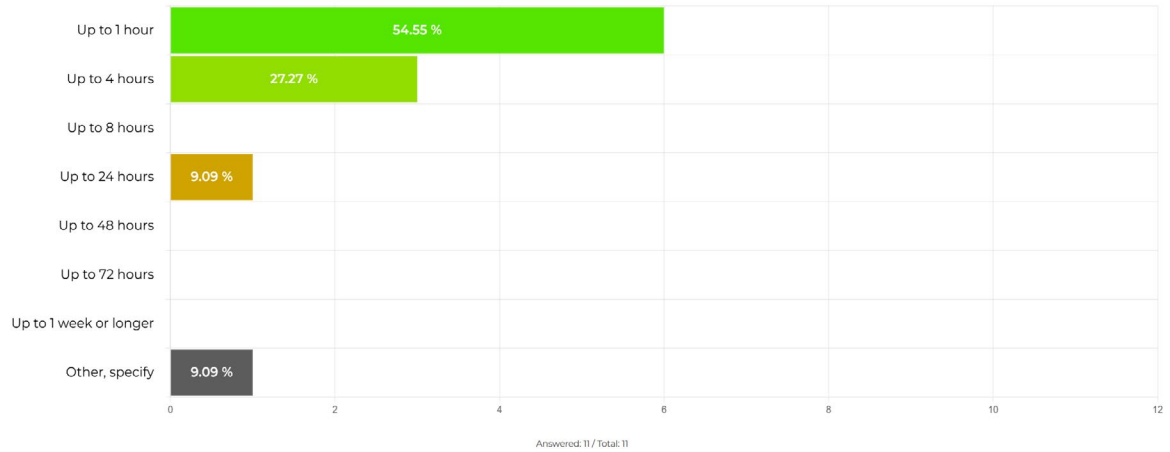
### 1.6 - ACCEPTABLE SERVICE DOWNTIME

What would be the acceptable service downtime for national critical energy infrastructure?



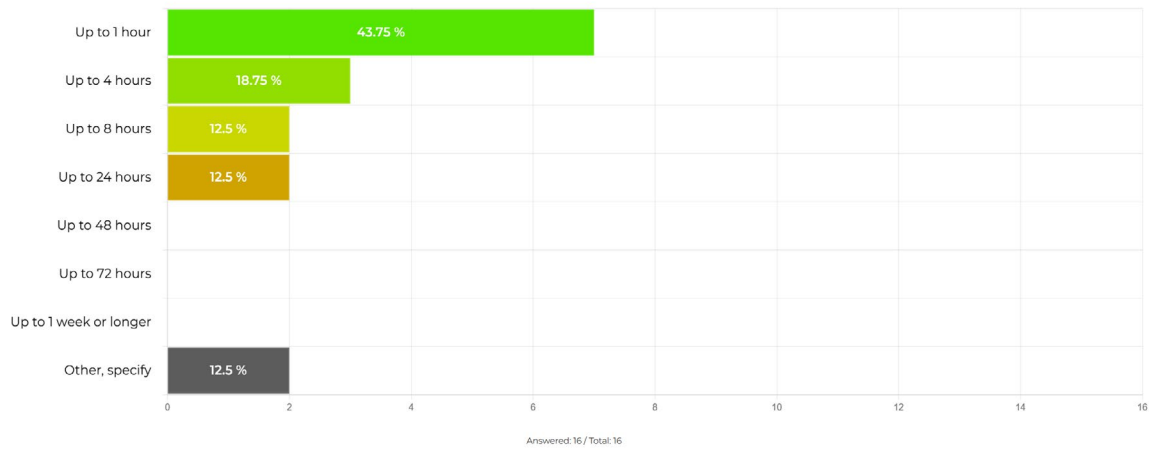
## 1.6 - ACCEPTABLE SERVICE DOWNTIME

What would be the acceptable service downtime for national critical energy infrastructure?



## 1.6 - ACCEPTABLE SERVICE DOWNTIME

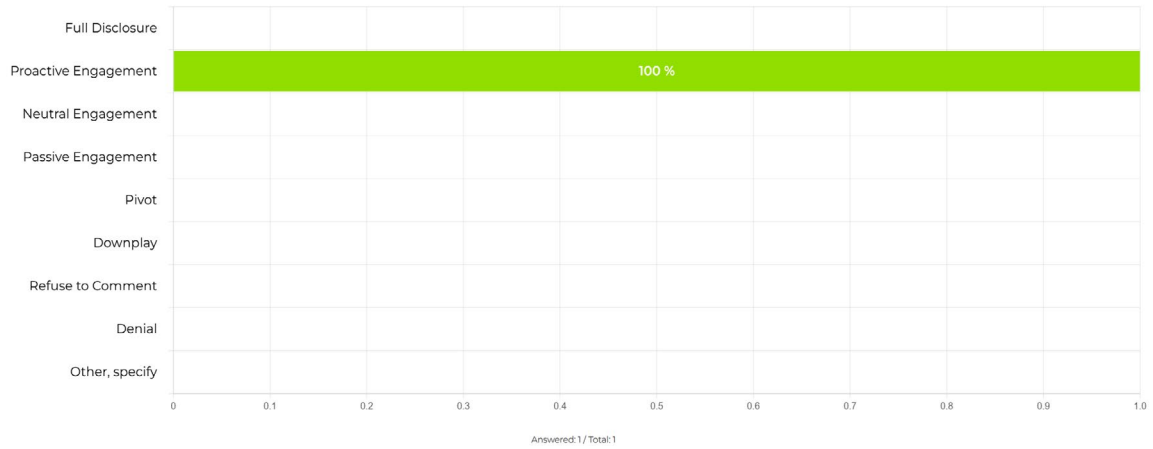
What would be the acceptable service downtime for national critical energy infrastructure?



WG3: Private Sector

### 1.5 - MEDIA STRATEGY

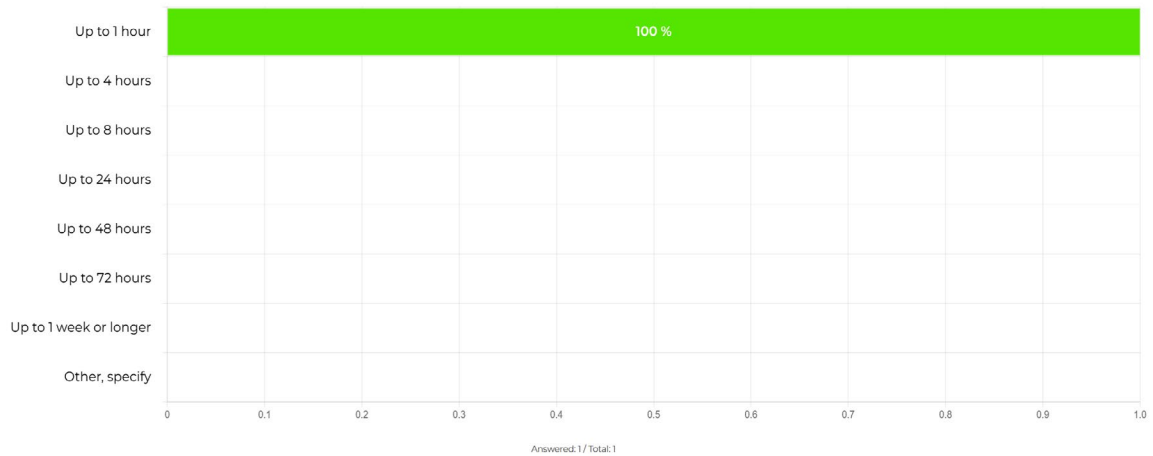
Please give a direction for the formulation of the official "lines to take" regarding the attacks:



WG4: Academia

### 1.6 - ACCEPTABLE SERVICE DOWNTIME

What would be the acceptable service downtime for national critical energy infrastructure?



### **Other, specify:**

- Depends on the specific CII (**Gen Gov05**)
- Only determined by your mean time to detect, respond, and repair (**Cyb Gov07**)
- National critical energy infrastructure should not have backup, e.g. financial services would mean losses (**Gen Gov09**)

### **Comments:**

- Will depend on BCP preparations for the energy sector (**Gen Gov14**) (**Up to 4 hours**)
- Restoration of services is necessary for economic activities to continue. Besides, the national crime rate may increase, especially if the outage happens at night. (**Academia01**) (**Up to 1 hour**)
- Banks aim for near-zero downtime (**Gen Gov08**) (**Up to 1 hour**)

## Inject 1.10 – ACADEMIA: PROVISION OF CYBERSECURITY EXPERTS

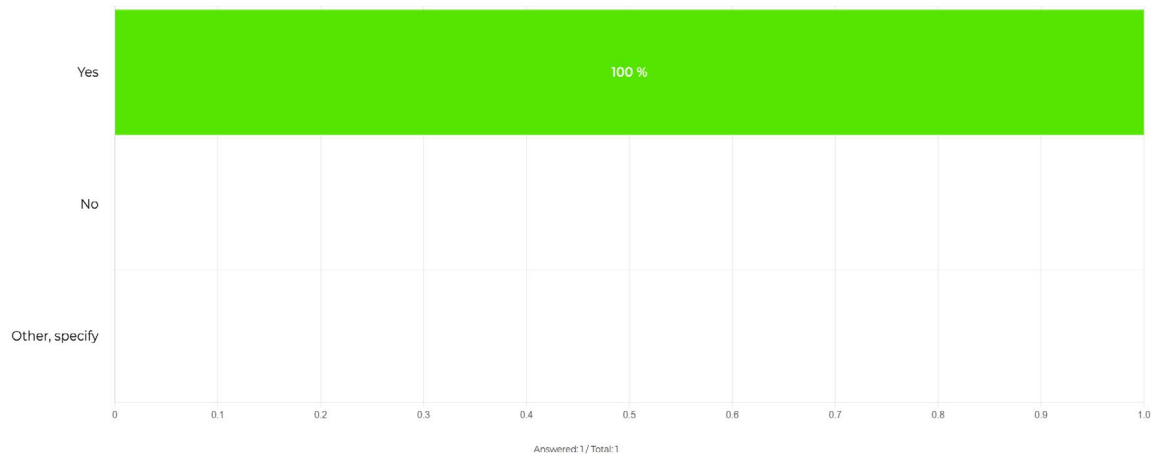
Do you support allocating cybersecurity experts to national authorities instead of daily responsibilities in response to the incident?

- Yes
- No
- Other, specify \_\_\_\_\_

WG4: Academia

### 1.10 - PROVISION OF CYBERSECURITY EXPERTS

Do you support allocating cybersecurity experts to national authorities instead of daily responsibilities in response to the incident?



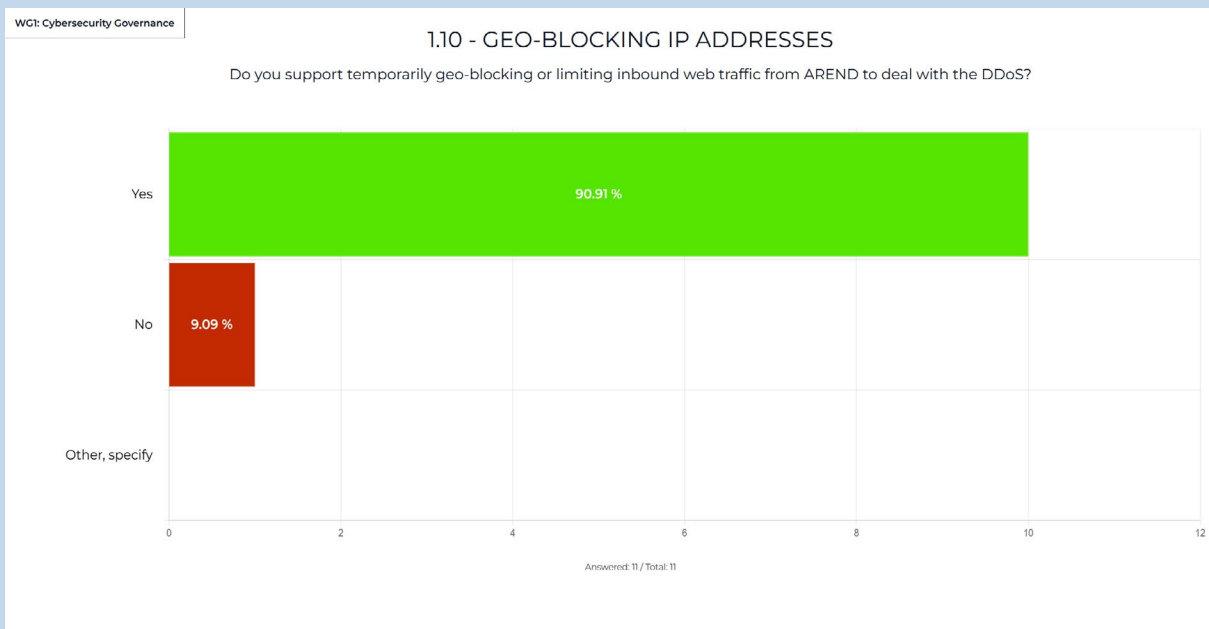
## Comments:

- Allocating resources to the national authorities would help in identifying the characteristics of the cyberthreat. Knowing the signatures of cyberthreats is a great advantage in prescribing future mitigation measures. **(Academia01) (Yes)**

## Inject 1.10 – CYBERSECURITY GOVERNANCE: GEO-BLOCKING IP ADDRESSES

Do you support temporarily geo-blocking or limiting inbound web traffic from AREND to deal with the DDoS?

- Yes
- No
- Other, specify \_\_\_\_\_



### Comments:

- Yes, this is a kind of rate limiting. This will sort the part where both affected nations can have **(Cyb Gov08) (Yes)**
- Although not a proper solution since the attacker might be using vpns, limiting traffic per ip might be helpful. **(Cyb Gov07) (Yes)**
- Since we have an idea of where the attack originated, I think it is safe to isolate the attack. **(Cyb Gov09) (Yes)**
- Because those are the traffic IPs that has been identified **(Cyb Gov10) (Yes)**

## Inject 1.10 – GENERAL GOVERNANCE: ENERGY REDUCTION

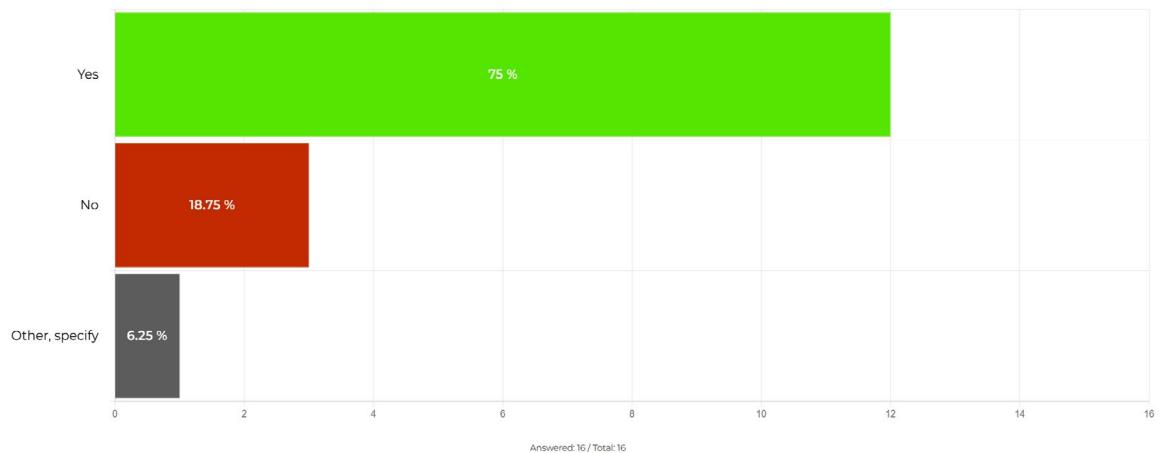
Do you support issuing a temporary national decree requiring a general reduction in energy usage?

- Yes
- No
- Other, specify \_\_\_\_\_

WG2: General Governance

### 1.10 - ENERGY REDUCTION

Do you support issuing a temporary national decree requiring a general reduction in energy usage?



### Other, specify:

- Hold the information to reduce the stress level and for crisis management as more credible information is sort as to what is happening (**Gen Gov13**)

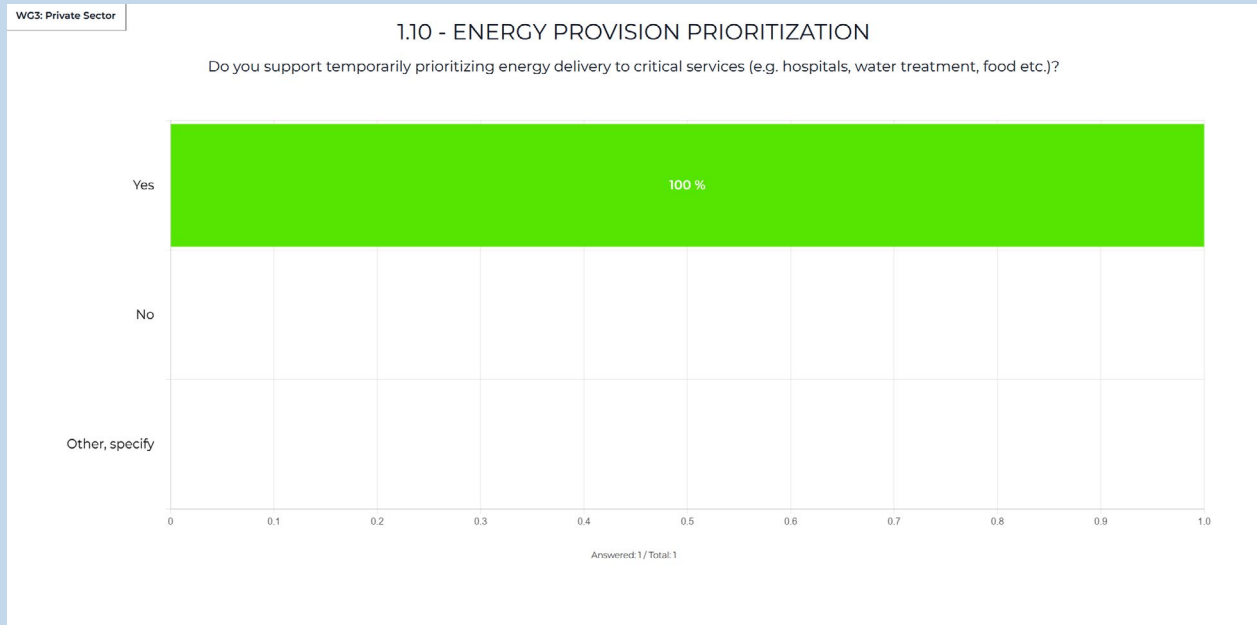
### Comments:

- Recommended in the situation regarding power consumption thresholds, outage notices etc. (**Gen Gov09, Yes**)

Inject 1.10 – PRIVATE SECTOR: ENERGY PROVISION PRIORITIZATION

Do you support temporarily prioritizing energy delivery to critical services (e.g. hospitals, water treatment, food, etc.)?

- Yes
- No
- Other, specify \_\_\_\_\_



## Inject 2.0 – SITUATION REPORT

After the numerous DDoS attacks on multiple KLAIDONIAN and WESPIAN energy service providers, a large-scale security review was put in place in KLAIDONIA as a safety mechanism to ensure no other threats remain in and against the systems.

One of the auditors discovers discrepancies in KLADOIL's DATACHAT SERVICE database – specific chat logs have been altered. The auditor does not make this information public, but quietly informs the responsible IT security officer, who brings in additional security service resources to analyse the situation.

Based on the complaint, a larger cyber threat hunting operation is launched. During the operation, a 0-day vulnerability in the "DATAFINE SYSTEMS" DATACHAT Software is discovered. The vulnerability runs a web-shell, a script that is typically used by complex state sponsored activities to exploit 0-day vulnerabilities. Through this vulnerability, the perpetrators have gained full privileges in the system and have complete "backdoor" access. The perpetrators act carefully but in recent days more active and reckless behavior is noted, probably the perpetrators act in anticipation of being discovered and a patch being issued.

As a result of the attack approximately 15% of the data in KLADOIL's DATACHAT software is inaccurate and the number is growing. A script – the nature of which is unclear – seems to have changed different chat records randomly and the logic of it is unclear. It is also unclear if the script has done anything else. It can be expected that other software DATAFINE SYSTEMS provides can also be compromised.

## Inject 2.1 – NOTIFICATION OBLIGATIONS

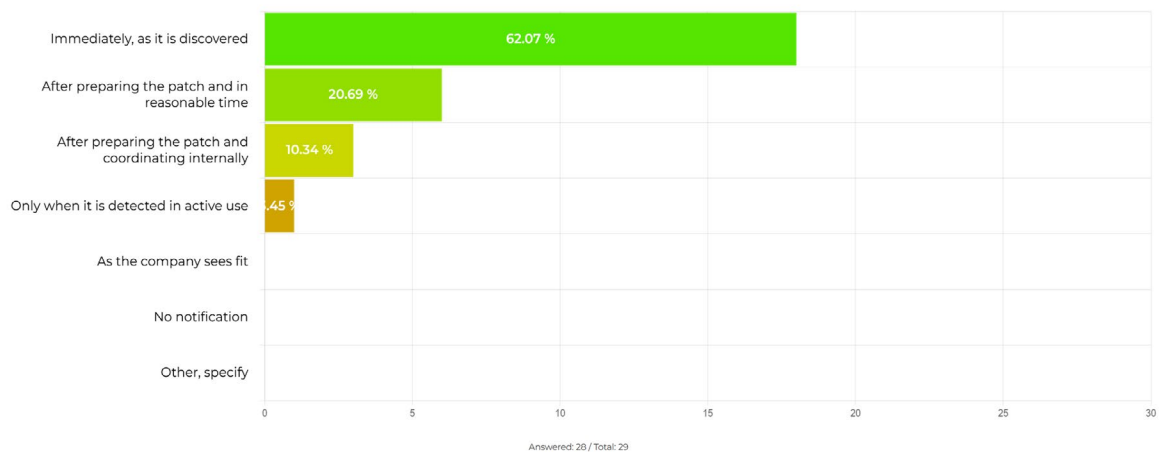
In situations like this, what should be KLADOIL's notification obligations to the national authorities about the vulnerability?

- Immediately, as it is discovered
- After preparing the patch and in reasonable time
- After preparing the patch and coordinating internally
- Only when it's detected in active use
- As the company sees fit
- No notification
- Other, specify \_\_\_\_\_

All

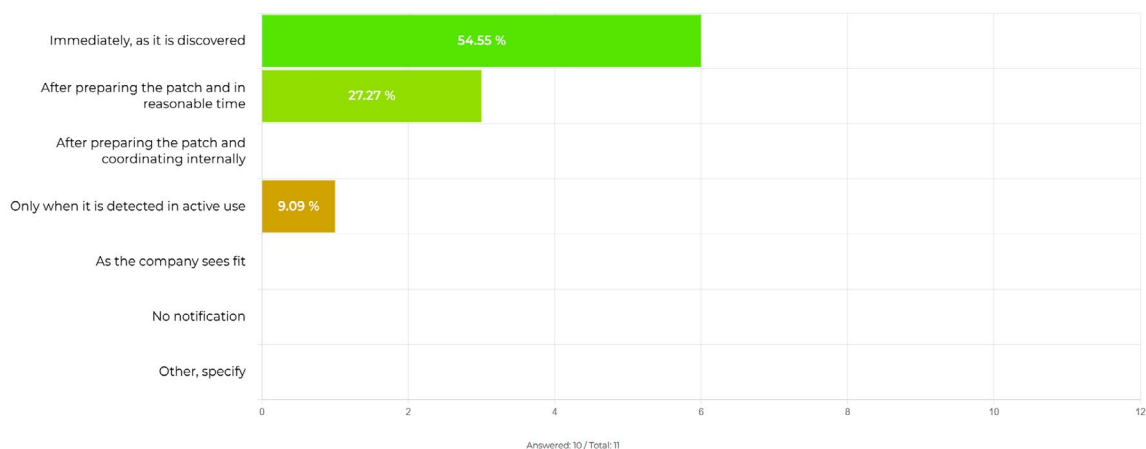
### 2.1 - NOTIFICATION OBLIGATIONS

In situations like this, what should be KLADOIL's notification obligations to the national authorities about the vulnerability?



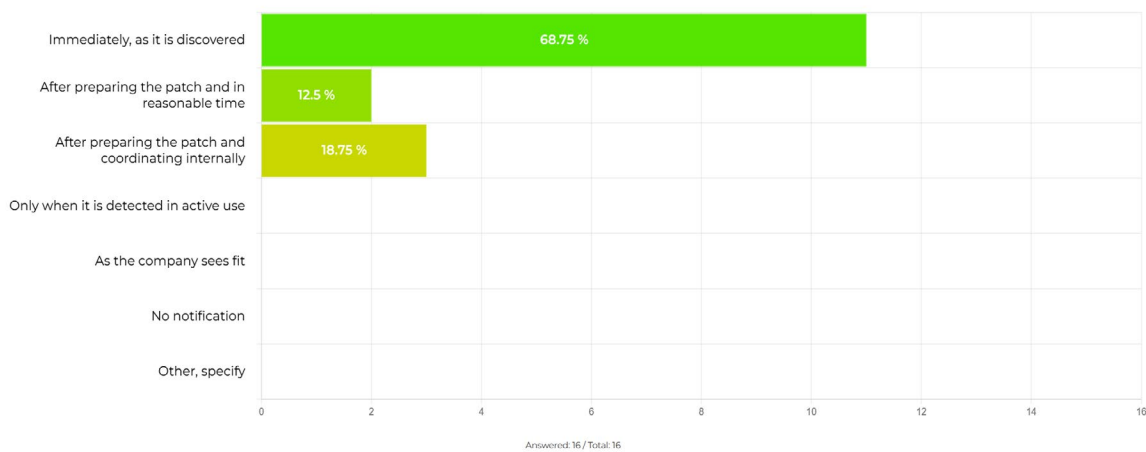
## 2.1 - NOTIFICATION OBLIGATIONS

In situations like this, what should be KLADOIL's notification obligations to the national authorities about the vulnerability?



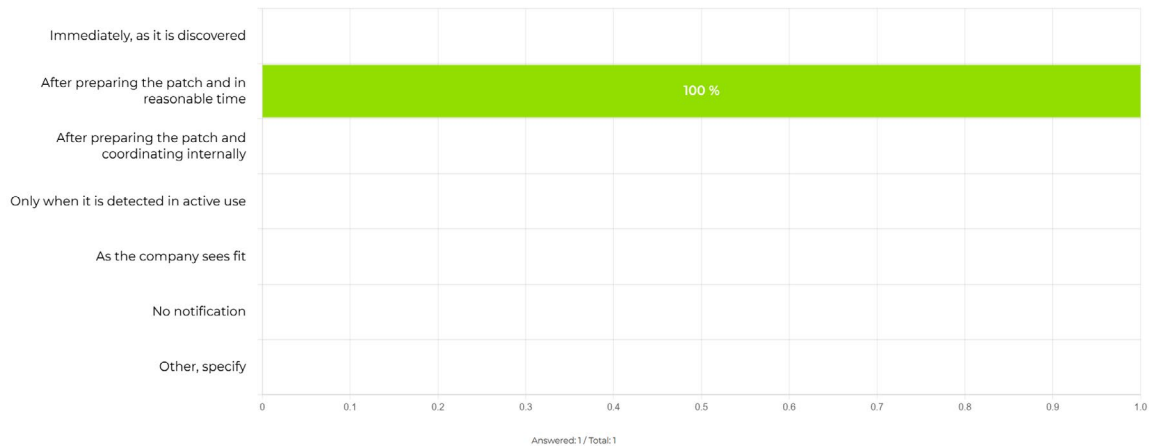
## 2.1 - NOTIFICATION OBLIGATIONS

In situations like this, what should be KLADOIL's notification obligations to the national authorities about the vulnerability?



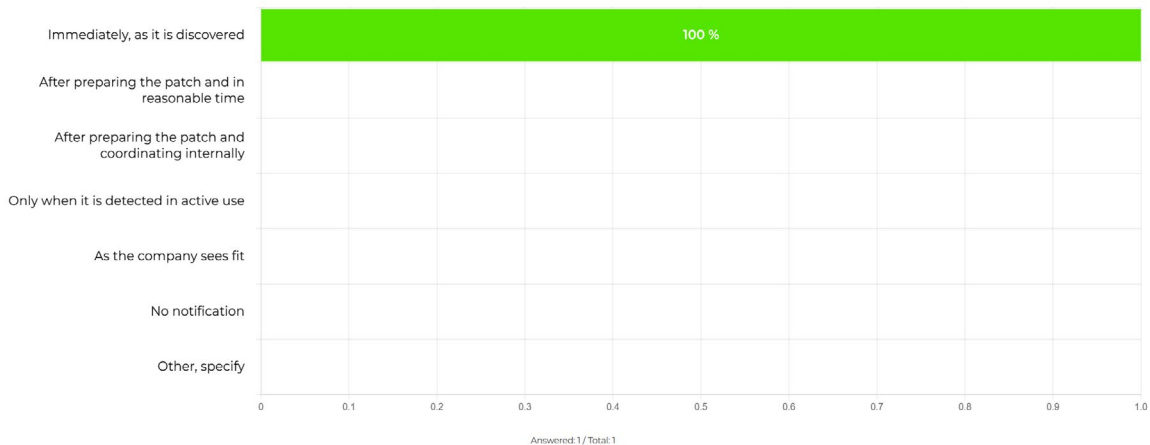
## 2.1 - NOTIFICATION OBLIGATIONS

In situations like this, what should be KLADOIL's notification obligations to the national authorities about the vulnerability?



## 2.1 - NOTIFICATION OBLIGATIONS

In situations like this, what should be KLADOIL's notification obligations to the national authorities about the vulnerability?



## Comments:

- Promptly notify the relevant national cybersecurity authorities (e.g., National CERT/CSIRT or sector regulator) as soon as the vulnerability is confirmed (**Cyb Gov08**) (**Immediately, as it is discovered**)
- This is to avoid maximum lateral movement and damage to the data and information in the information systems. (**Academia01**) (**Immediately, as it is discovered**)

## Inject 2.4 – INFORMATION SECURITY POLICY

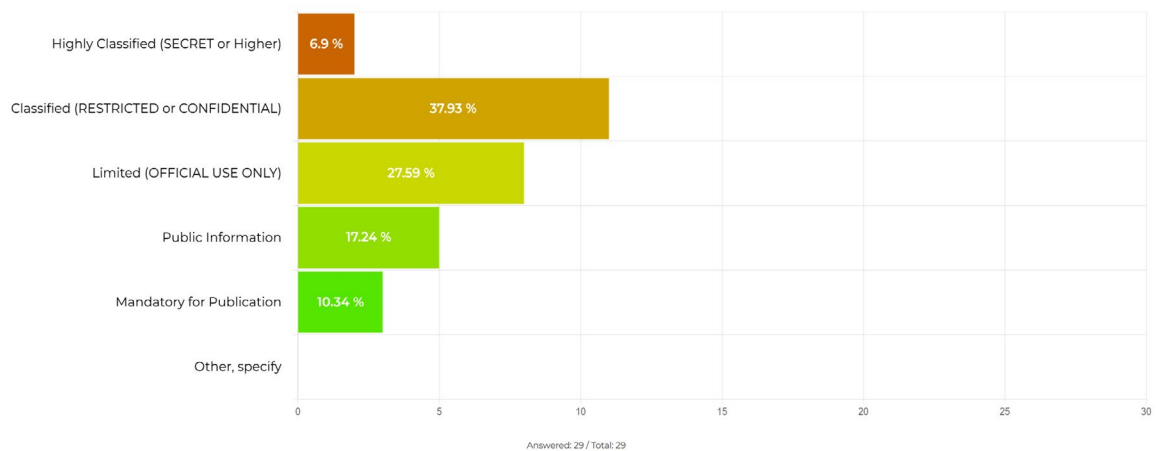
In your opinion, should the decision about the 0-day vulnerability be public knowledge or classified? Define the level of classification of this information.

- Highly Classified (SECRET or Higher)
- Classified (RESTRICTED or CONFIDENTIAL)
- Limited (OFFICIAL USE ONLY)
- Public Information
- Mandatory for Publication
- Other, specify \_\_\_\_\_

All

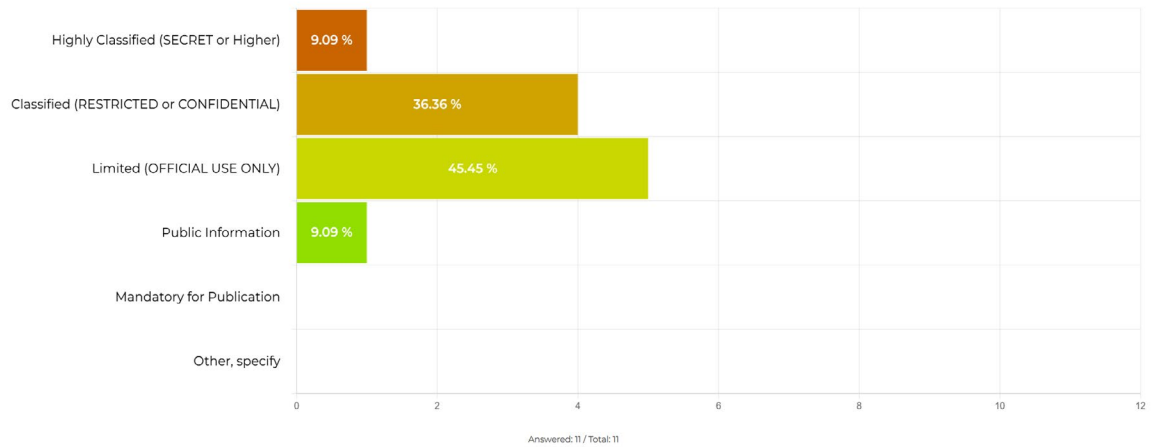
### 2.4 - INFORMATION SECURITY POLICY

In your opinion, is the decision about the 0-day vulnerability public knowledge or classified? Define the level of classification of this information.



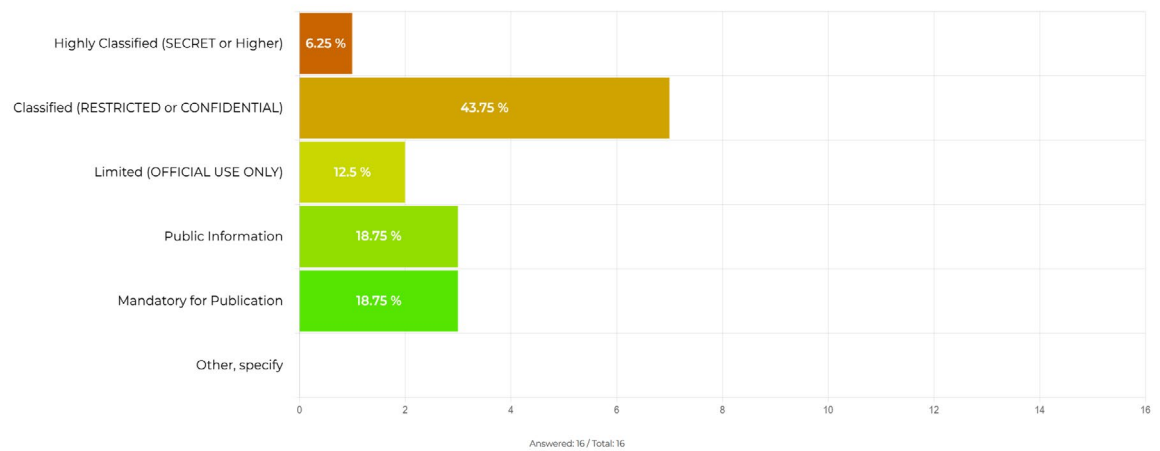
## 2.4 - INFORMATION SECURITY POLICY

In your opinion, is the decision about the 0-day vulnerability public knowledge or classified? Define the level of classification of this information.



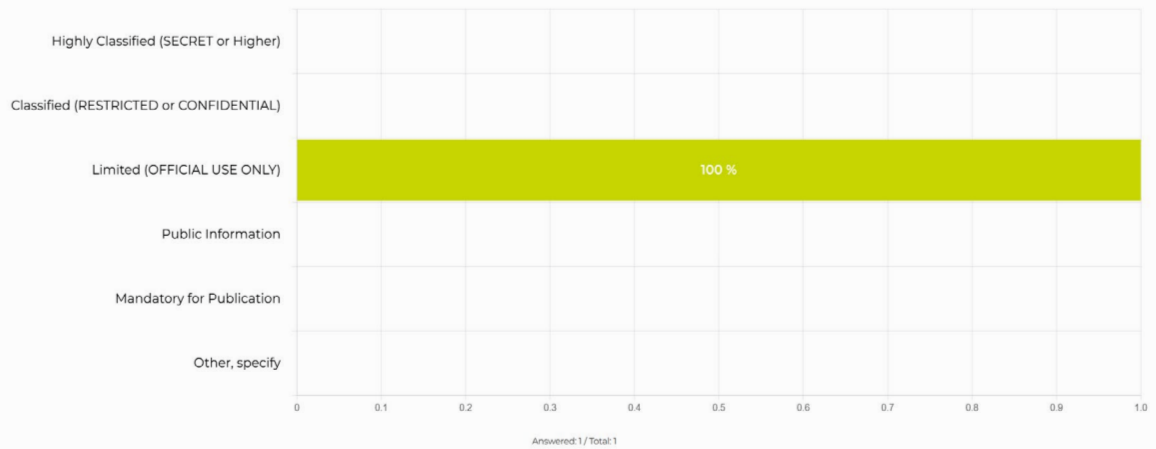
## 2.4 - INFORMATION SECURITY POLICY

In your opinion, is the decision about the 0-day vulnerability public knowledge or classified? Define the level of classification of this information.



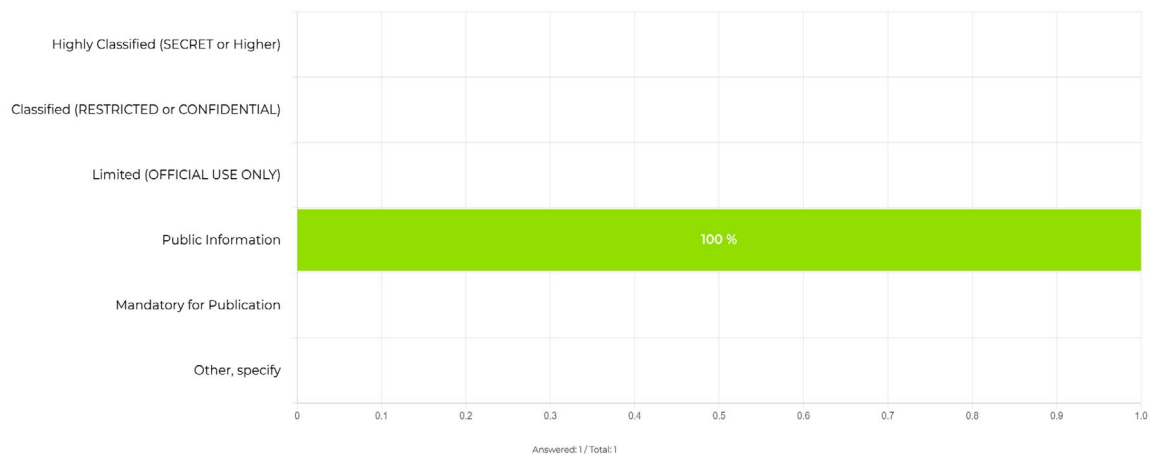
## 2.4 - INFORMATION SECURITY POLICY

In your opinion, is the decision about the 0-day vulnerability public knowledge or classified? Define the level of classification of this information.



## 2.4 - INFORMATION SECURITY POLICY

In your opinion, is the decision about the 0-day vulnerability public knowledge or classified? Define the level of classification of this information.



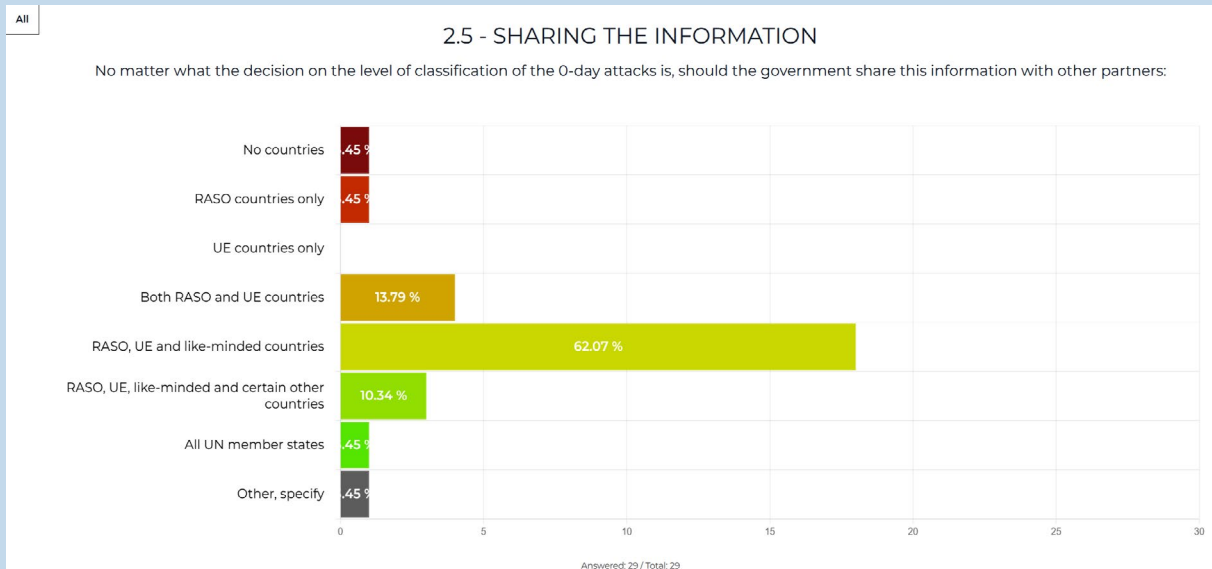
## Comments:

- The decision about a 0-day vulnerability is not public knowledge unless officially disclosed. (Cyb Gov08) (Classified - RESTRICTED OR CONFIDENTIAL)

## Inject 2.5 – SHARING THE INFORMATION

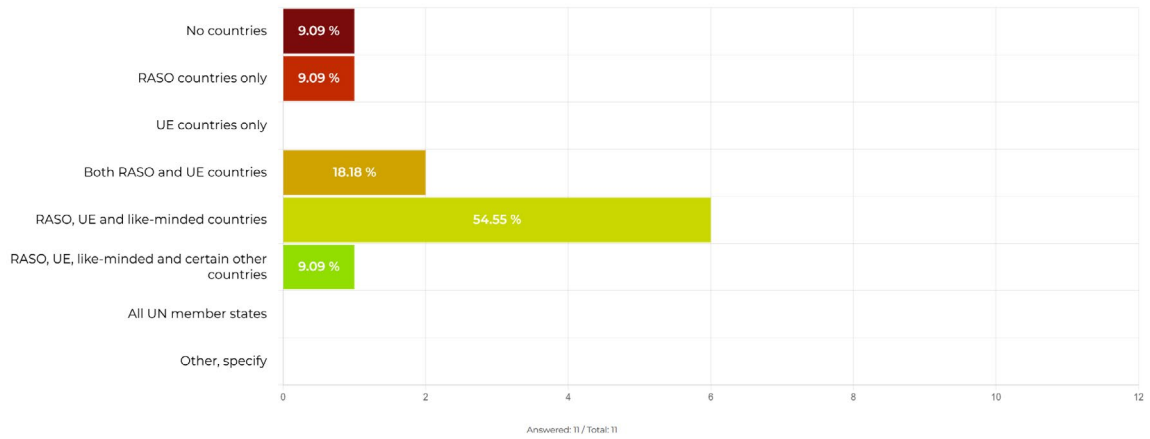
No matter what the decision on the level of classification of the 0-day attacks is, should the government share this information with other partners:

- No countries
- RASO countries only
- UE countries only
- Both RASO and UE countries
- RASO, UE and, like-minded countries
- RASO, UE, like-minded, and certain other countries
- All UN member states
- Other, specify \_\_\_\_\_



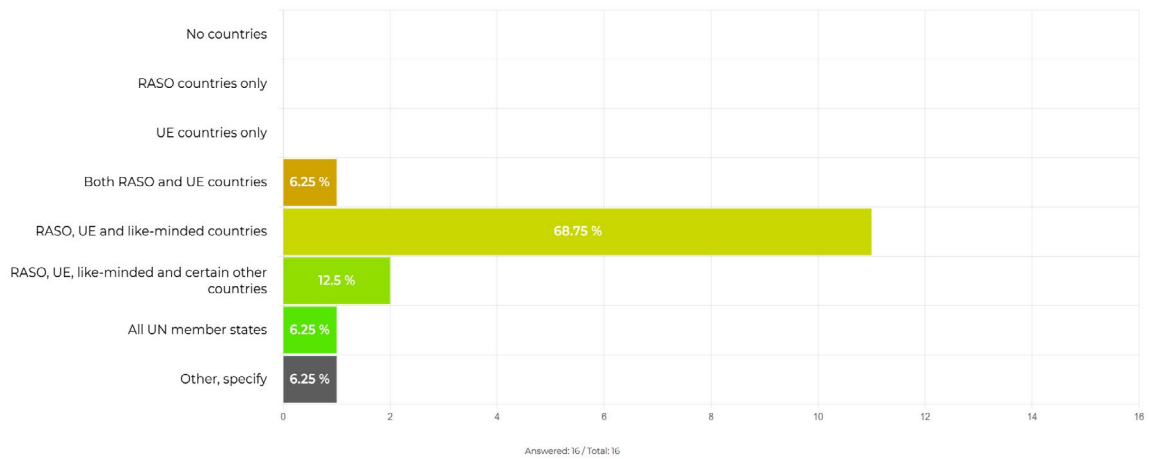
## 2.5 - SHARING THE INFORMATION

No matter what the decision on the level of classification of the 0-day attacks is, should the government share this information with other partners:



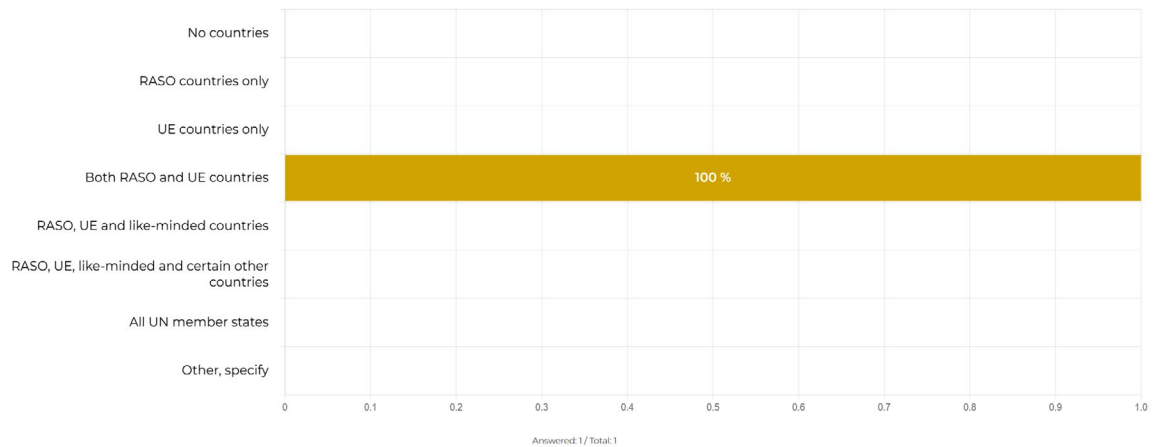
## 2.5 - SHARING THE INFORMATION

No matter what the decision on the level of classification of the 0-day attacks is, should the government share this information with other partners:



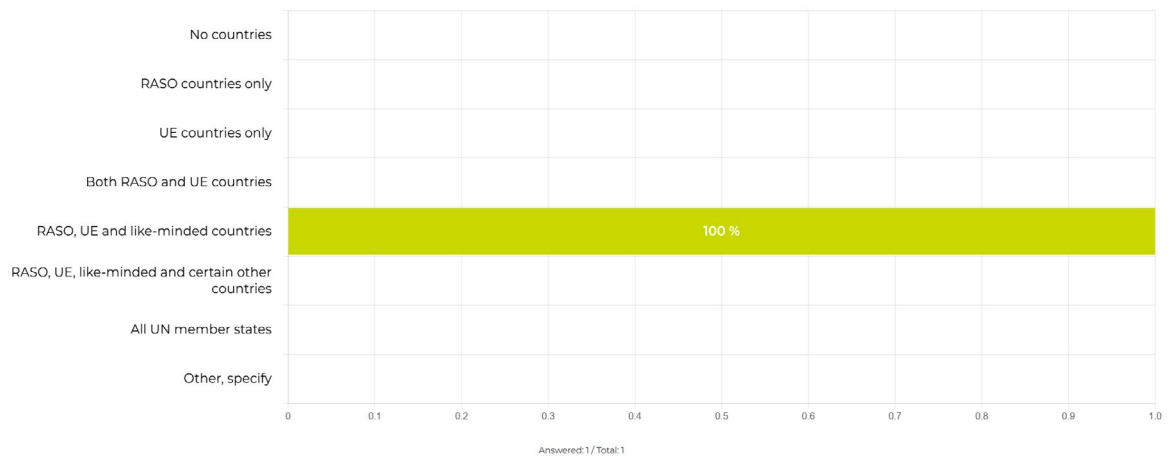
## 2.5 - SHARING THE INFORMATION

No matter what the decision on the level of classification of the 0-day attacks is, should the government share this information with other partners:



## 2.5 - SHARING THE INFORMATION

No matter what the decision on the level of classification of the 0-day attacks is, should the government share this information with other partners:



### Other, specify:

- All countries (Gen Gov2)

## Inject 3.5 – SITUATION UPDATE

Dear Customer:

You have been selected as a “voluntary” subject of the Angry Turtle New Encryption Service Beta Test.

As you are reading this message, it can be said that the Beta Test has been successful and we thank you for your participation and contribution.

In order to continue normal operations, we kindly request you to transfer 17 BTC to the following wallet address:  
1Lbcfr7sAHTD9CgdQo3HTMTkV8LK4ZnX71

In return you will receive:

- A loyalty membership spot in our beta testing service repository
- A decryption package to un-do the effects of the beta test and continue your operations

The deadline for the payment is 5 days.

To contact us for further details, please write an official statement with your reference number (PT-2821) to the address  
helpdesk-angryturtle@protonmail.com

- *Angry Turtle*

**KLAFIN** reports that its core banking systems have come under cyber-attack. The primary target of the attack is critical commercial service infrastructure. The nature of the attack is encryption malware. As a precaution, KLAFIN has decided to halt operation of the entire system. This is done over the abundance of concern that the attackers maybe have obtained information, allowing them to further carry out attacks on vulnerable parts of the network.

Internally, no additional information currently exists on how and from where the perpetrators gained access to the systems and if any other systems or services are compromised.

The following details have been confirmed according to the ransom note:

- The attacker group is ANGRY TURTLE APT (associated with CRONUNG), which is a notorious and internationally known ransomware formation
- Although a state sponsored organization, they are mostly financially motivated in delivering ransomware
- According to the “core values” of ANGRY TURTLE, they provide a decryption key for every payment, ensuring, that this is a part of their “business model” to maintain a “good” reputation
- ANGRY TURTLE also has a “helpdesk” which can be used to contact them in different payment-related questions

- The perpetrators have set a ransom demand of 17BTC, amounting to roughly 230 MLN KES.
- The attackers have stolen nearly 100 gigabytes of data and are threatening to release it on the internet if the ransom is not paid

**KLAFIN** has been unsuccessful in restoring the information from backups.

### Inject 3.6 – RANSOMWARE PREPAREDNESS MEASURES

From the perspective of your Working Group, please indicate what are the key elements Critical Infrastructure providers should have in their ransomware risk management and preparedness plans?

#### **CYBERSECURITY GOVERNANCE:**

- Data Protection and Backup Strategy, Technical Preventive Controls, and Comprehensive Risk Assessment (**Cyb Gov04**)
- Communications channels Backups System infrastructure documentation Cyber threat intelligence channels Policies, strategies Government oversight and collaboration methods Effective and efficient cybersecurity tools (**Cyb Gov07**)
- Incidence Response Frameworks Cyber Security Policies e.g. Business Continuity (**Cyb Gov08**)
- The companies likely to suffer such attacks should invest in secure backup cloud systems (**Cyb Gov13**)
- 3-2-1 backup rule Have a risk register (**Cyb Gov06**)
- Create a structured checklist template (e.g., governance, prevention, detection, response, recovery) that you can adapt. (**Cyb Gov10**)
- Critical Infrastructure providers must have strong governance, clear roles, and defined decision-making authority for ransomware incidents. They need well defined preventive controls, including network segmentation, MFA, EDR, and secure, tested offline backups etc A dedicated ransomware response and recovery plan, supported by regular exercises, is essential. Crisis communication procedures and ensure coordination with national CERT, regulators, and key partners. (**Cyb Gov03**)
- IR and Recovery Plans/Procedures - Proper BCP (**Backup (tested)**) (**Cyb Gov14**)

- a.) 3-2-1 backup strategy b.) Ransomware use cases (playbooks, run books etc.) embedded into the SOC framework **(Cyb Gov02)**
- Create a structured checklist template (e.g., governance, prevention, detection, response, recovery) that you could adapt. **(Cyb Gov10)**
- Updated Ransomware Playbook **(Cyb Gov01)**

#### **GENERAL GOVERNANCE:**

- SECURE BACK UPS CLEAR INTERNAL AND EXTERNAL COMMS CHANNELS **(Gen Gov2)**
- Upto date backups **(Gen Gov03)**
- Clear communication channel - Defined roles and responsibilities - Risk insurance **(Gen Gov05)**
- Always have money at your disposal to pay ransom in case of ransomware attack **(Gen Gov07)**
- Timely patching of systems, have an offsite backup **(Gen Gov08)**
- Working backup plans **(Gen Gov01)**
- Business continuity management /operations; with back up and disaster recovery options **(Gen Gov13)**
- Air gapped backups -Anti-ransomware capable EDR **(Gen Gov15)**
- Comprehensive ransomware playbooks that are updated and tested regularly. These include having information security policies, IR plans, backup plans, among others. **(Gen Gov06)**
- Set up an offline backup of your systems. Install regular backups. MFA, Employee awareness, risk policy **(Gen Gov09)**
- Contacts with Authorities, **(Gen Gov04)**
- User Training on detecting phishing techniques **(Gen Gov15)**
- Negotiate when possible **(Gen Gov11)**
- Need for offline backups, and redundant network of critical entities such as health, energy, and finance **(Gen Gov10)**
- Have proper back-ups in place **(Gen Gov12)**
- Have a clear BCP plan in place **(Gen Gov12)**

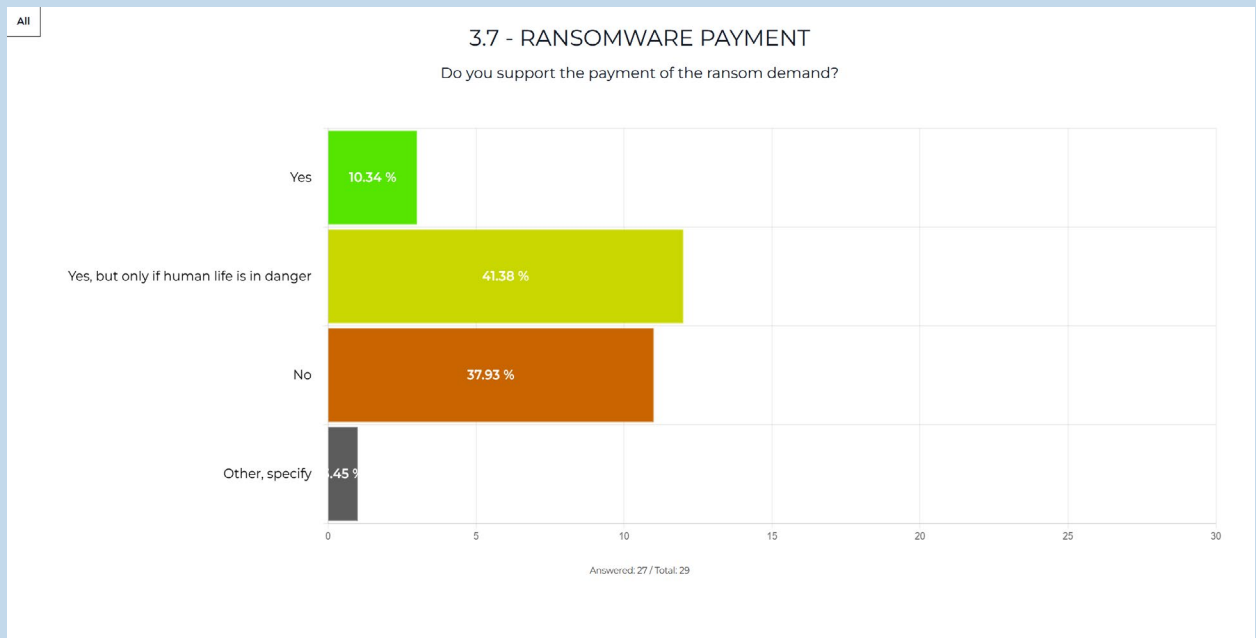
#### **CIVIL SOCIETY & ACADEMIA**

- 1. Install and operationalize a Security Incident and Event Management (SIEM) System. 2. Install an Endpoint Detection and Response (EDR). 3. Install a malware detection system. 4. Implement a robust Security Operations Centre (SOC) to detect, protect, respond and recover from cybersecurity incidents. **(Academia01)**

### Inject 3.7 – RANSOMWARE PAYMENT

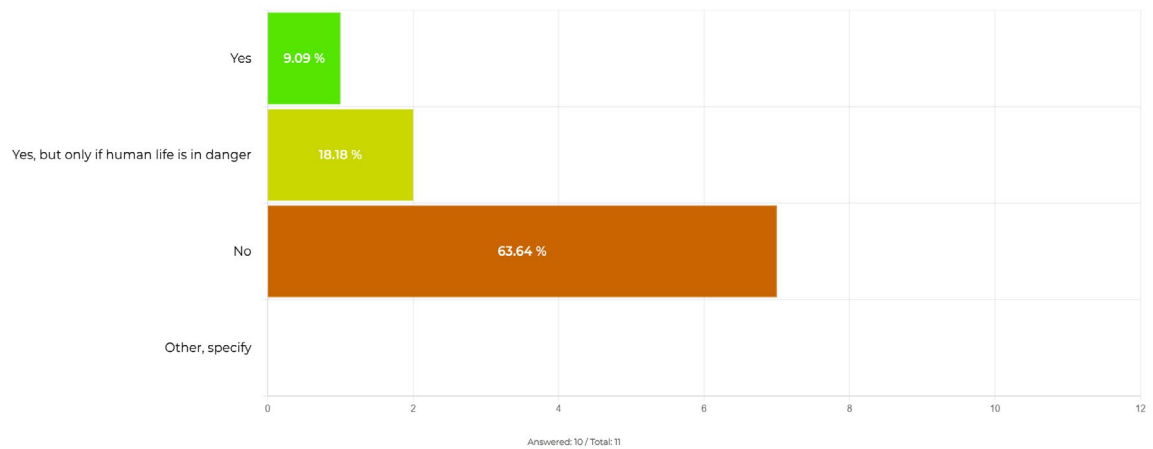
Do you support the payment of the ransom demand?

- Yes
- Yes, but only if human life is in danger
- No
- Other, specify \_\_\_\_\_



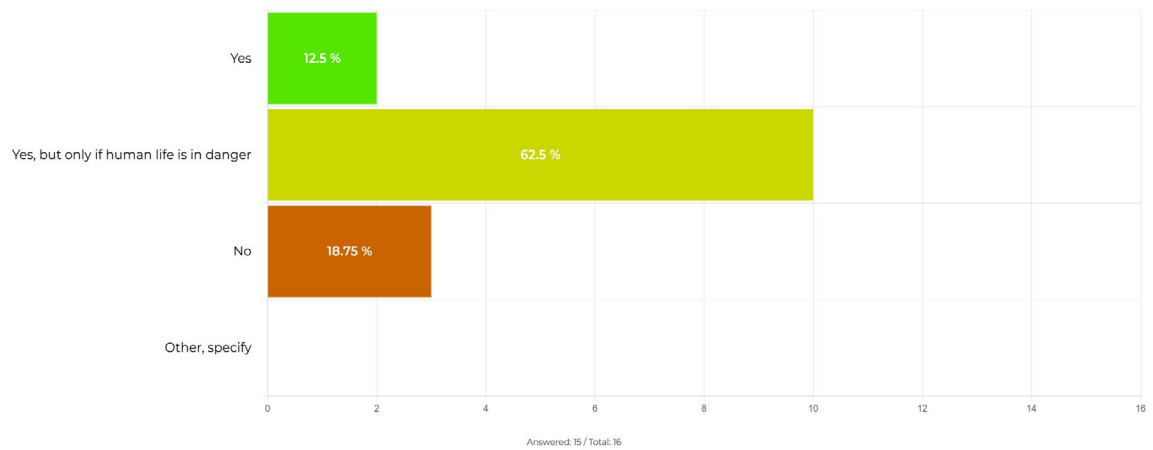
## 3.7 - RANSOMWARE PAYMENT

Do you support the payment of the ransom demand?



## 3.7 - RANSOMWARE PAYMENT

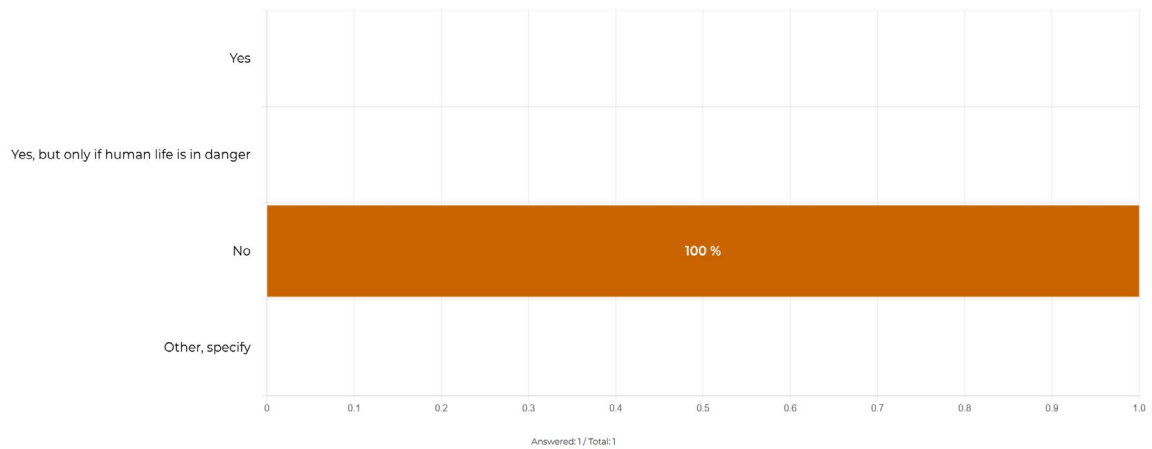
Do you support the payment of the ransom demand?



WG3: Private Sector

### 3.7 - RANSOMWARE PAYMENT

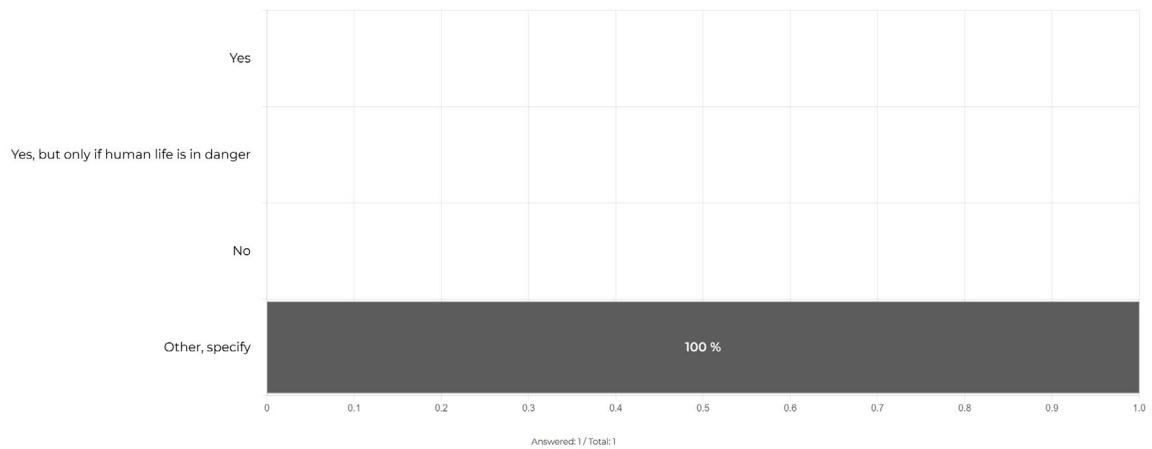
Do you support the payment of the ransom demand?



WG4: Academia

### 3.7 - RANSOMWARE PAYMENT

Do you support the payment of the ransom demand?



### Other, specify:

- Dependent on the type of data involved (**Academia01**)
- No but you may not have a choice (**Cyb Gov14**)

### Comments:

- Human life takes precedence during information security incidence response (**Gen Gov04**) (**Yes, but only if human life is in danger**)

## Inject 3.7.1 – DECISION-MAKING FRAMEWORK

In the context of the preceding decision:

1) How much time in applying all relevant rules and regulations of KLAIDONIA do you realistically estimate it would take in a real-life situation to reach a decision? Please give your most realistic opinion.

- Less than 1 hour
- 1-4 hours
- Up to 12 hours
- Up to 1 week
- 1-3 weeks
- 1 month
- 3 months
- 6 months
- 1 year
- More than 1 year

2) In your opinion, is the decision public or classified? If classified, please indicate the level of classification. If the term is different from the choices below, specify by choosing option other.

- Top Secret (keyword)
- Top Secret

- Secret
- Confidential
- Restricted
- Company confidential
- Official use only
- Unclassified
- For publication
- Mandatory for Publication

3) What cooperation network (national or international) is needed?

- National decision, one agency
- National decision but several agencies
- National decision, involving also private sector
- Select allies/partners
- 1 regional organization
- 2 or more regional organizations
- Regional organizations + "trusted partners"
- Regional organizations, "Trusted partners" and private sector
- Beyond regional organizations and "trusted partners"
- Beyond regional organizations and "trusted partners" + private sector

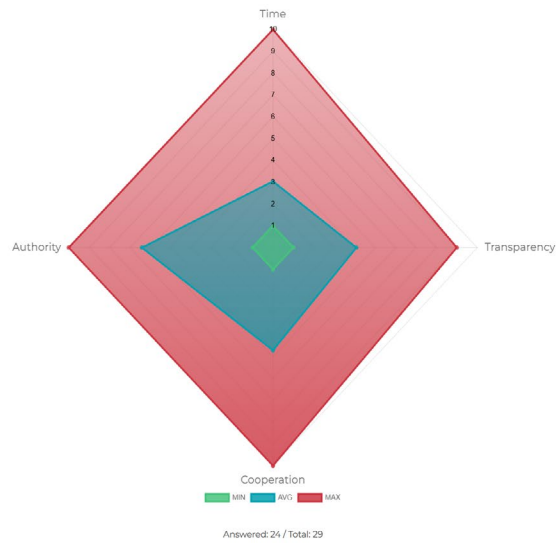
4) Who (what authority) is ultimately authorised to take this decision? The examples below are general – please pick the closest or choose option other and specify the actual authority who fits best.

- Administrator, Expert, Official / Account manager, customer service
- Senior Civil Servant / Head of a small Business Unit
- Head of Unit / Head of a larger business unit
- Head of Department / Head of major Business Unit
- Most Senior Civil Servant / Company CEO
- Committee of Senior Civil Servants / Group Level Executive
- Minister / CEO – Group Level
- Ministerial Committee / Board of Supervisors
- Cabinet of Ministers / Shareholders' meeting
- Parliament

All

### 3.7.1 - DECISION-MAKING FRAMEWORK

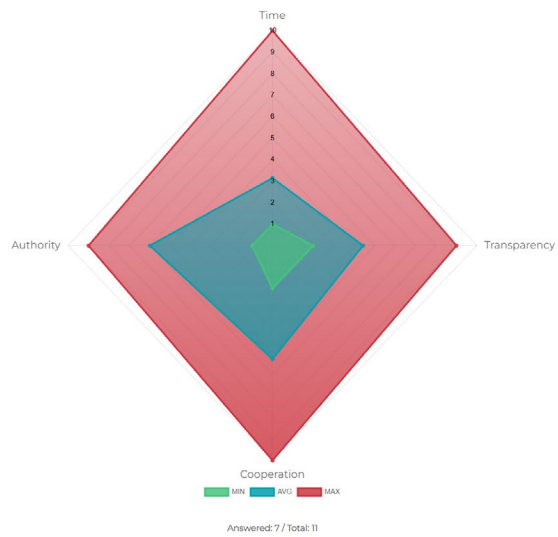
In the context of the preceding decision:



WG: Cybersecurity Governance

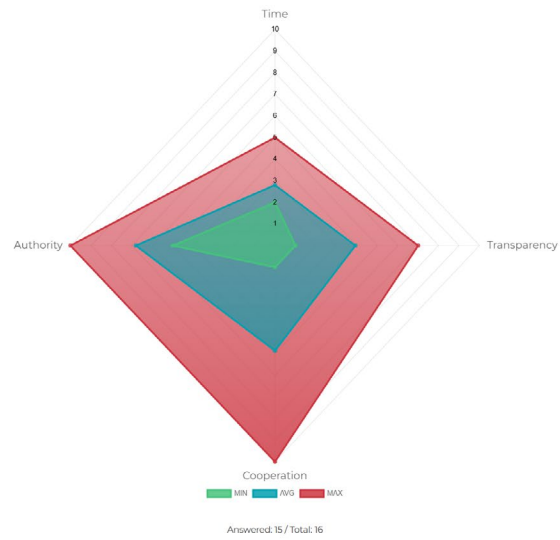
### 3.7.1 - DECISION-MAKING FRAMEWORK

In the context of the preceding decision:



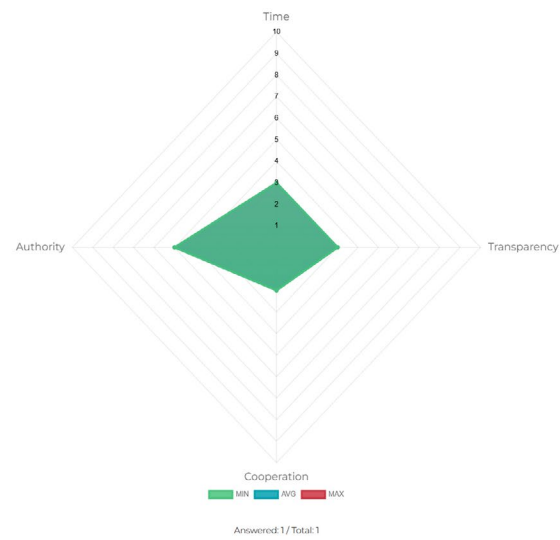
### 3.7.1 - DECISION-MAKING FRAMEWORK

In the context of the preceding decision:



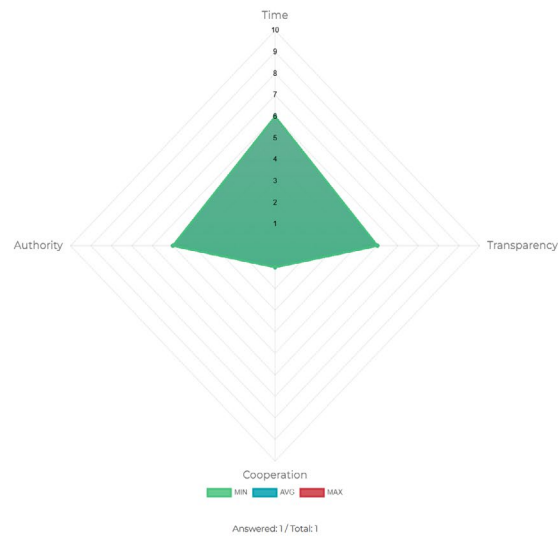
### 3.7.1 - DECISION-MAKING FRAMEWORK

In the context of the preceding decision:



## 3.7.1 - DECISION-MAKING FRAMEWORK

In the context of the preceding decision:



## Comments:

- The CEO is the accounting officer answerable in all affairs decision making. (Cyb Gov13) **(Up to 12 hours, Confidential, National decision but several agencies, Most Senior Civil Servant / Company CEO)**

## Inject 3.8 – NEGOTIATION ≠ PAYMENT?

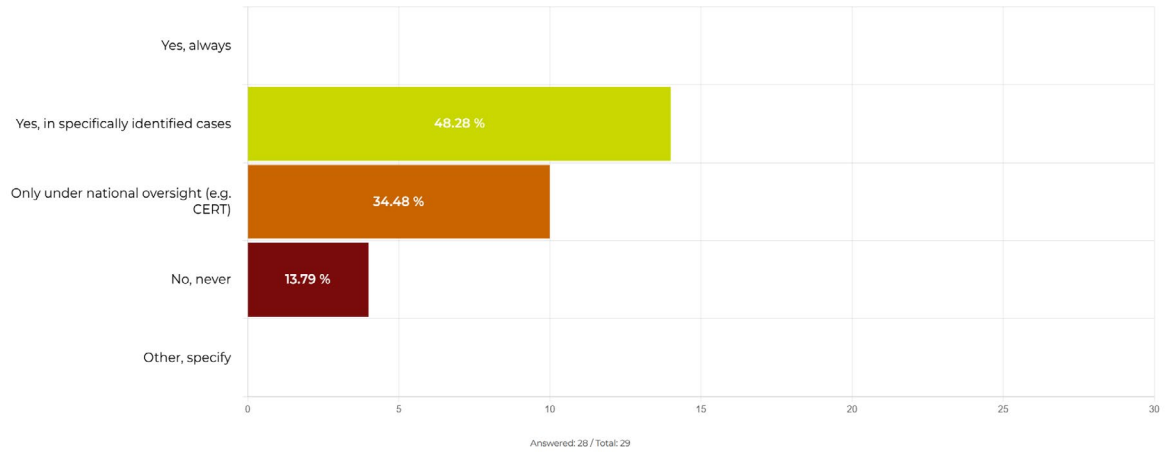
Should government agencies or critical infrastructure operators be allowed to open communication channels with ransomware actors, even under no-payment policies?

- Yes, always
- Yes, in specifically identified cases
- Only under national oversight (e.g. CERT)
- No, never
- Other, specify \_\_\_\_\_

All

### 3.8 - NEGOTIATION ≠ PAYMENT?

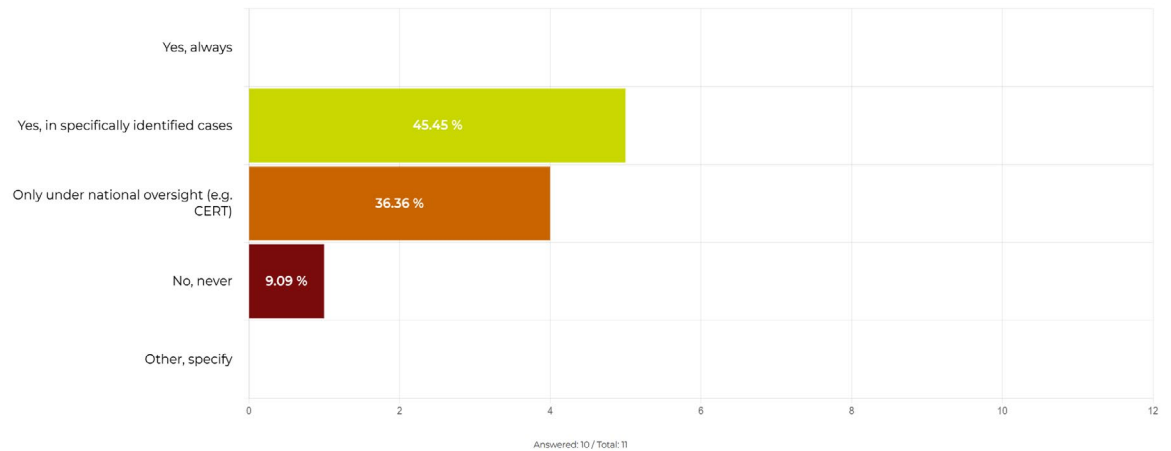
Should government agencies or critical infrastructure operators be allowed to open communication channels with ransomware actors, even under no-payment policies?



WGI: Cybersecurity Governance

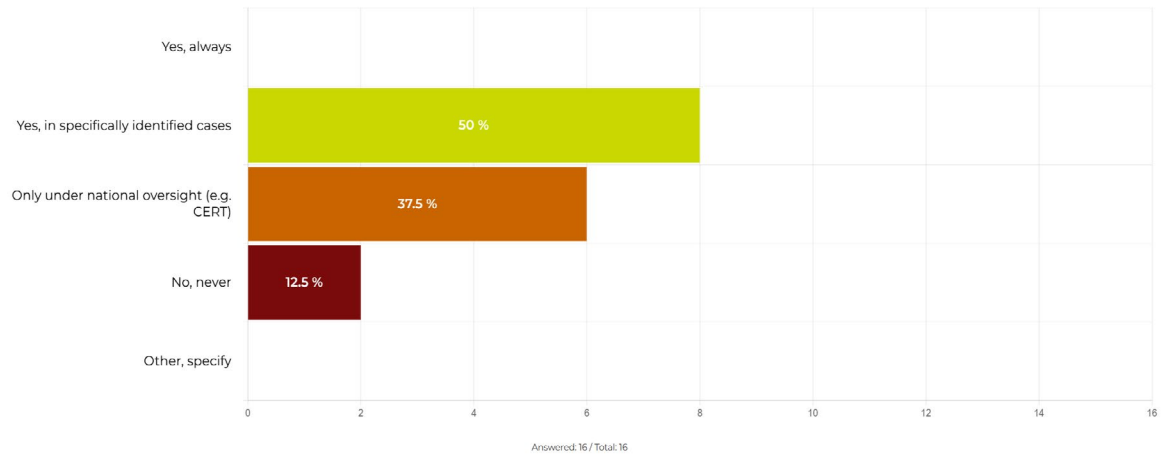
### 3.8 - NEGOTIATION ≠ PAYMENT?

Should government agencies or critical infrastructure operators be allowed to open communication channels with ransomware actors, even under no-payment policies?



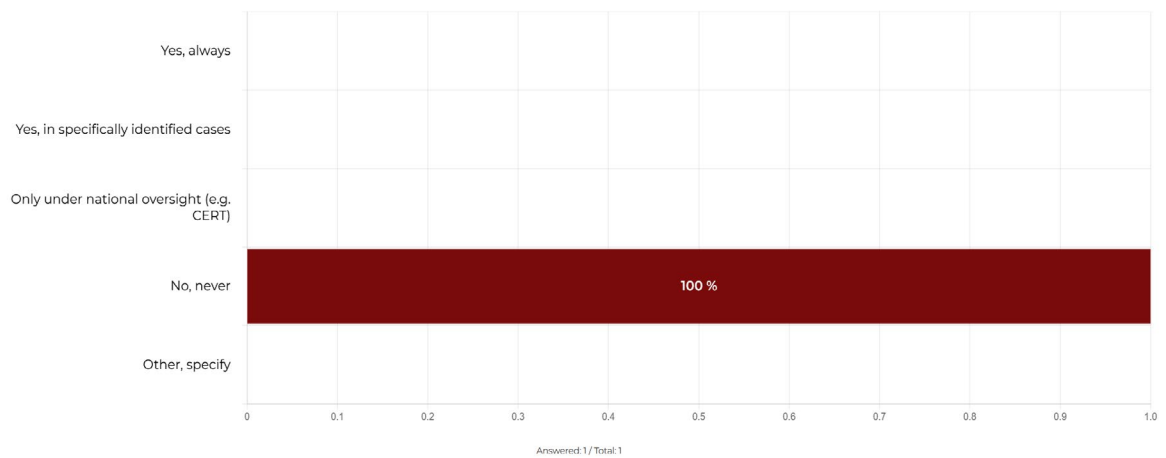
### 3.8 - NEGOTIATION ≠ PAYMENT?

Should government agencies or critical infrastructure operators be allowed to open communication channels with ransomware actors, even under no-payment policies?



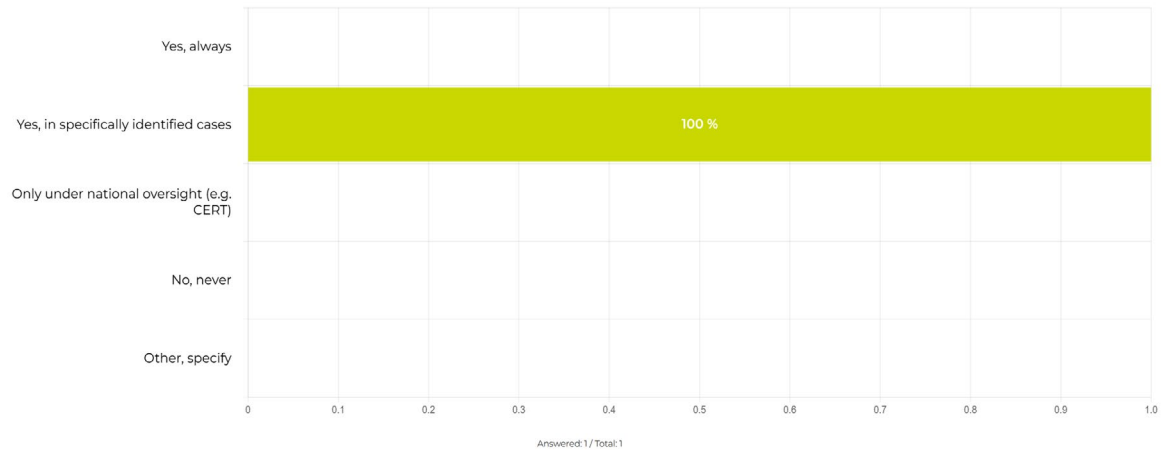
### 3.8 - NEGOTIATION ≠ PAYMENT?

Should government agencies or critical infrastructure operators be allowed to open communication channels with ransomware actors, even under no-payment policies?



## 3.8 - NEGOTIATION ≠ PAYMENT?

Should government agencies or critical infrastructure operators be allowed to open communication channels with ransomware actors, even under no-payment policies?



### Comments:

- On case-by-case basis (Cyb Gov10) (Only under national oversight (e.g. CERT))
- Looking at the impact of loss of data and severity of the situation (Academia01) (Yes, in specifically identified cases)

## Inject 4.2 – SECTORAL PRIORITIZATION IN A CYBER CATASTROPHE

The Critical Entities Resilience Directive lays down obligations on EU Member States to take specific measures to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market.

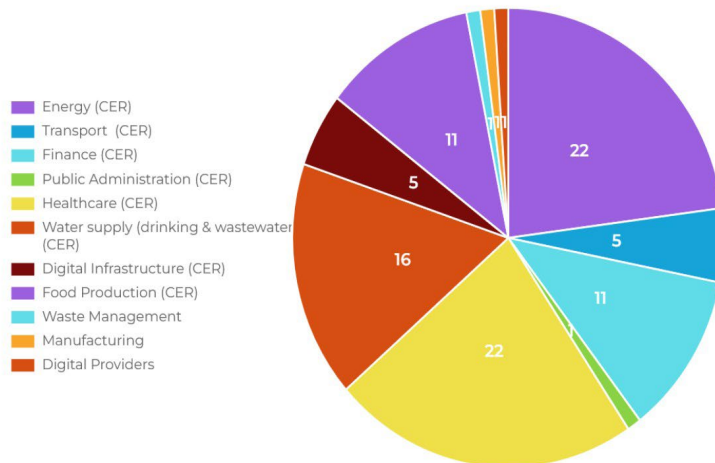
Please indicate the 4 most critical sectors in ensuring a functioning society while keeping in mind also the CER Directive:

- Energy (CER)
- Transport (CER)
- Finance (CER)
- Public Administration (CER)
- Healthcare (CER)
- Space (CER)
- Water supply (drinking & wastewater) (CER)
- Digital Infrastructure (CER)
- Food Production (CER)
- Postal Services
- Waste Management
- Chemicals
- Research
- Manufacturing
- Digital Providers
- Other (please specify)

All

#### 4.2 - SECTORAL PRIORITIZATION IN A CYBER CATASTROPHE

Please indicate the 4 most critical sectors in ensuring a functioning society while keeping in mind also the CER Directive:

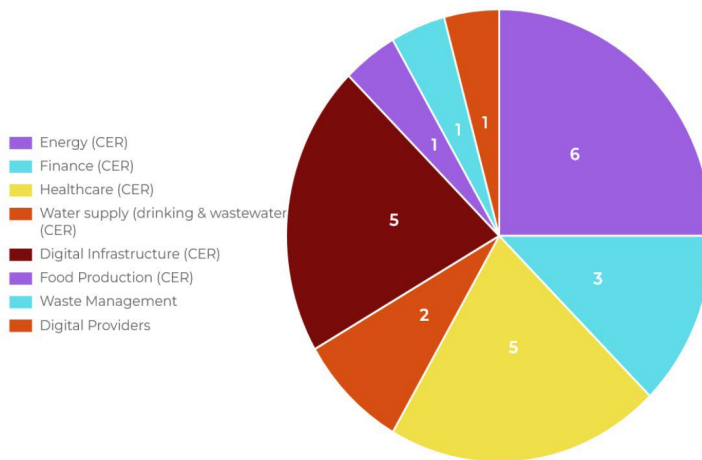


Answered: 24 / Total: 29

WGI: Cybersecurity Governance

#### 4.2 - SECTORAL PRIORITIZATION IN A CYBER CATASTROPHE

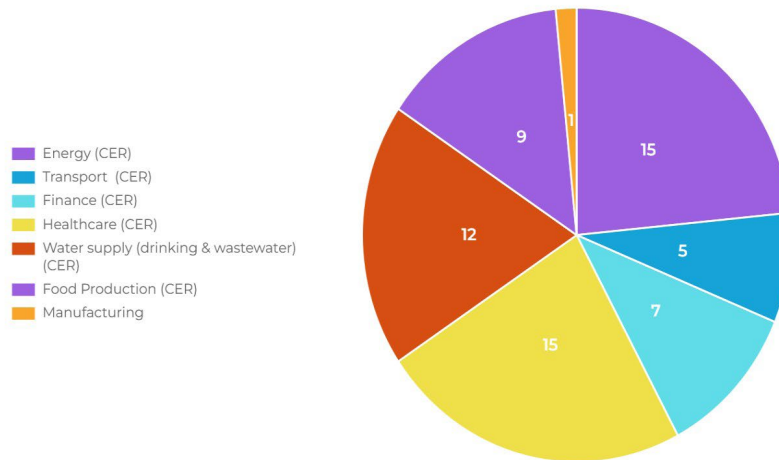
Please indicate the 4 most critical sectors in ensuring a functioning society while keeping in mind also the CER Directive:



Answered: 6 / Total: 11

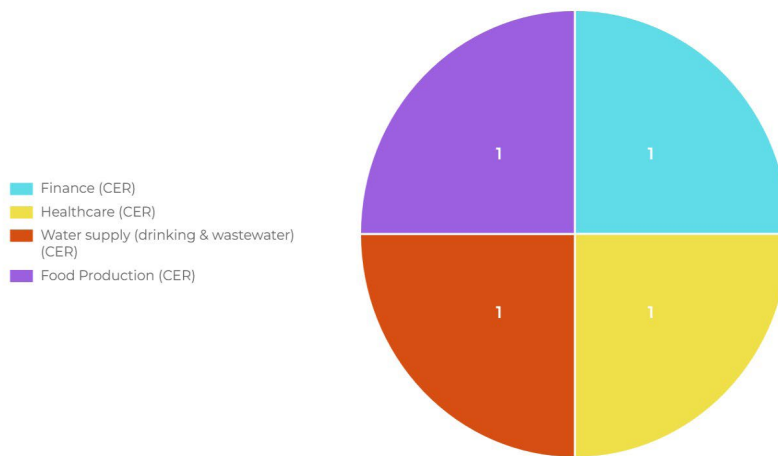
## 4.2 - SECTORAL PRIORITIZATION IN A CYBER CATASTROPHE

Please indicate the 4 most critical sectors in ensuring a functioning society while keeping in mind also the CER Directive:



## 4.2 - SECTORAL PRIORITIZATION IN A CYBER CATASTROPHE

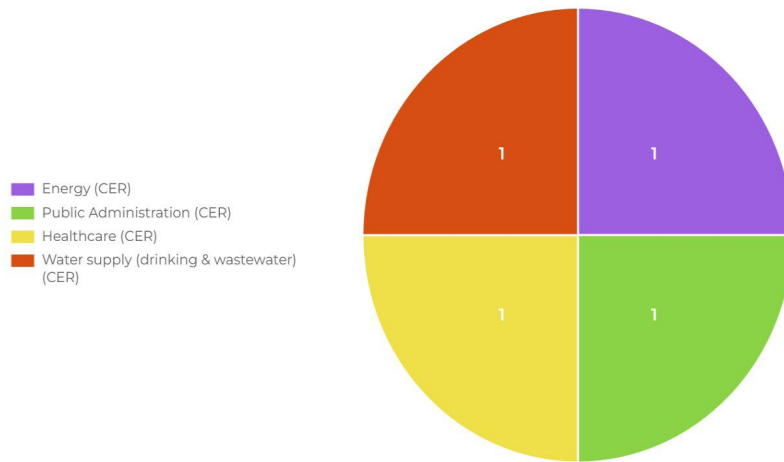
Please indicate the 4 most critical sectors in ensuring a functioning society while keeping in mind also the CER Directive:



Answered: 1 / Total: 1

## 4.2 - SECTORAL PRIORITIZATION IN A CYBER CATASTROPHE

Please indicate the 4 most critical sectors in ensuring a functioning society while keeping in mind also the CER Directive:

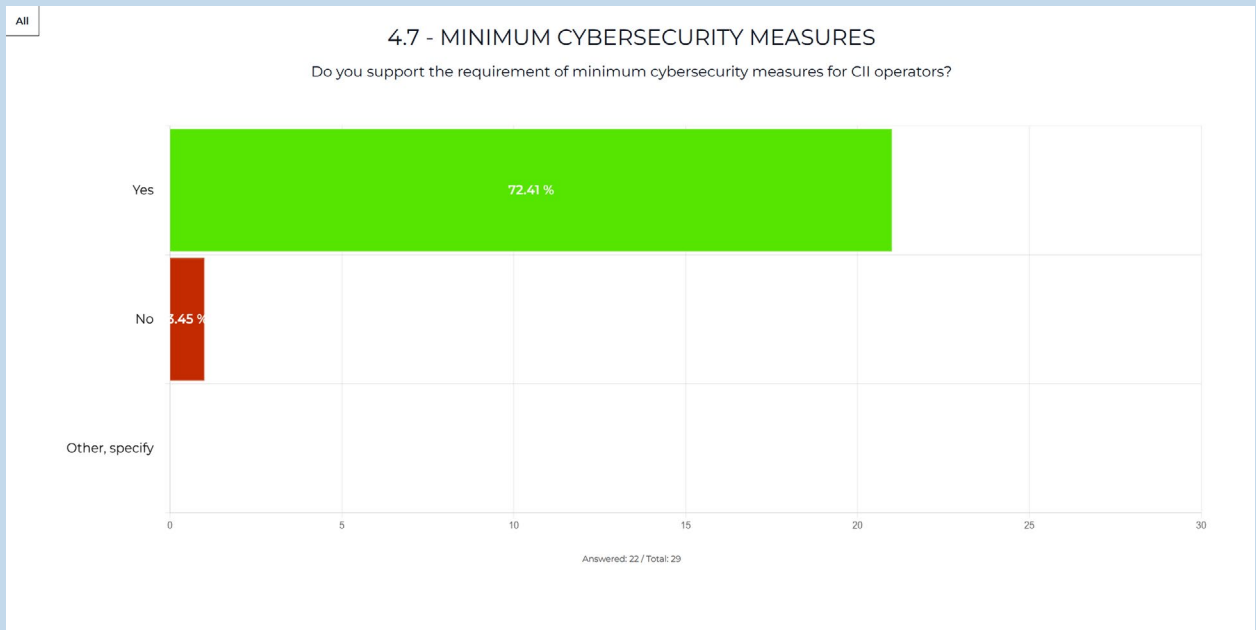


Answered: 1 / Total: 1

Inject 4.7 – MINIMUM CYBERSECURITY MEASURES

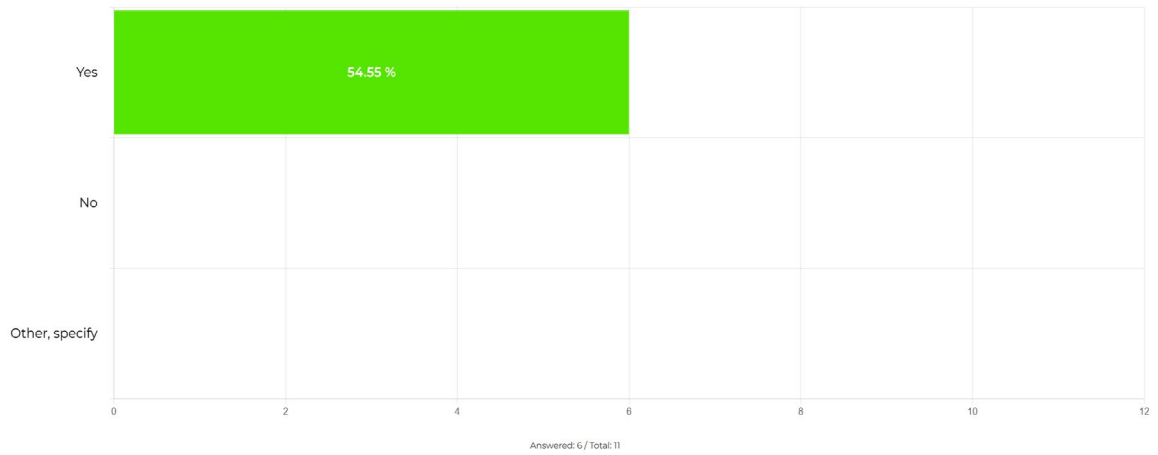
Do you support the requirement of minimum cybersecurity measures for CII operators?

- Yes
- No
- Other, specify \_\_\_\_\_



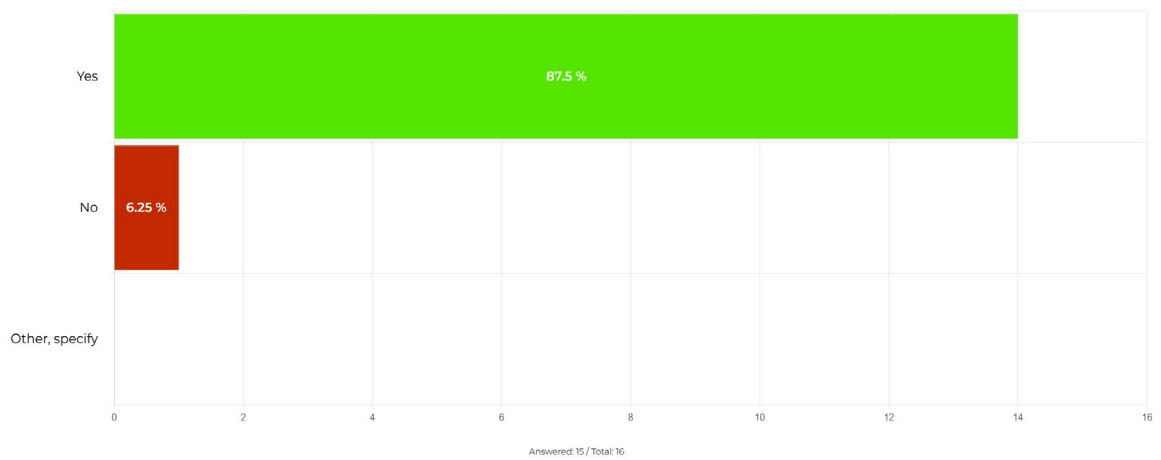
## 4.7 - MINIMUM CYBERSECURITY MEASURES

Do you support the requirement of minimum cybersecurity measures for CII operators?



## 4.7 - MINIMUM CYBERSECURITY MEASURES

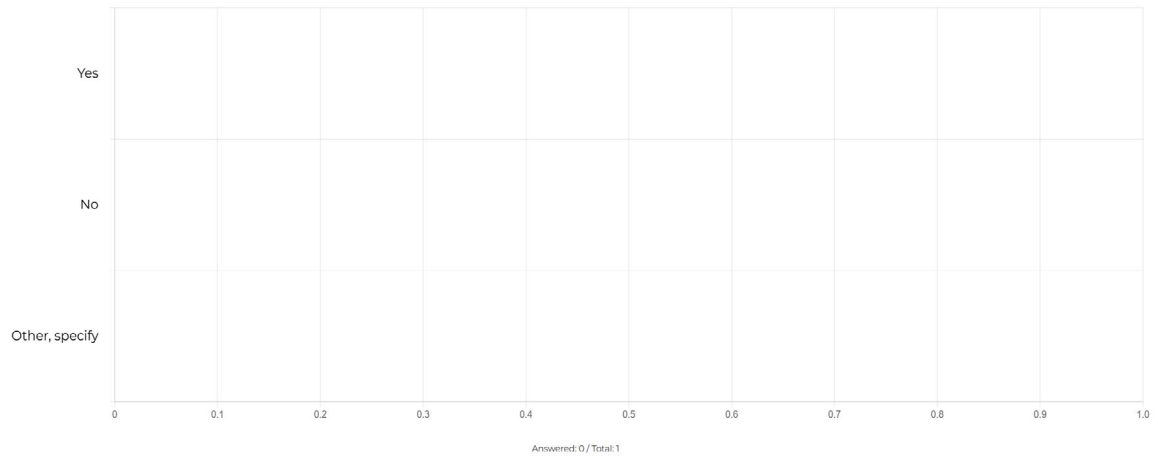
Do you support the requirement of minimum cybersecurity measures for CII operators?



WG3: Private Sector

#### 4.7 - MINIMUM CYBERSECURITY MEASURES

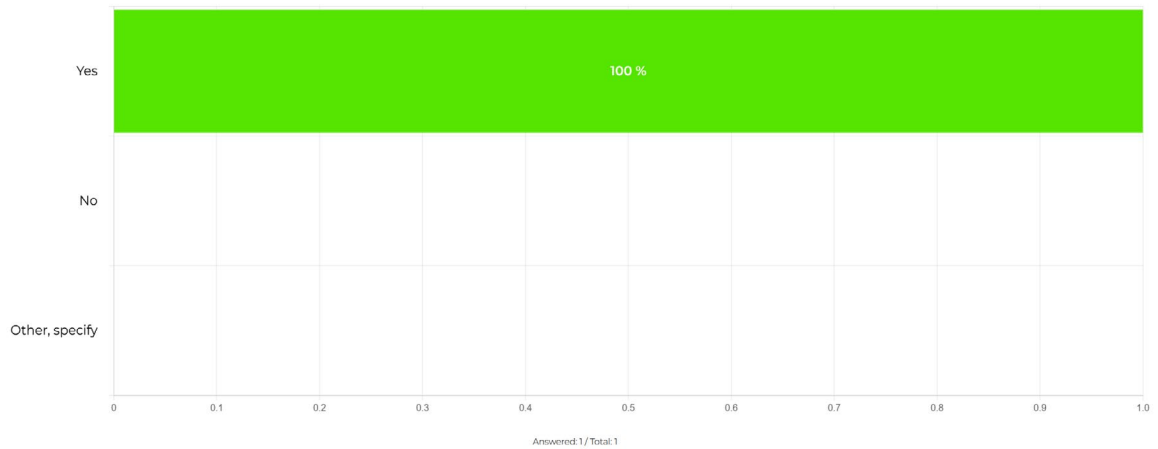
Do you support the requirement of minimum cybersecurity measures for CII operators?



WG4: Academia

#### 4.7 - MINIMUM CYBERSECURITY MEASURES

Do you support the requirement of minimum cybersecurity measures for CII operators?



## Comments:

- Define minimum cyber hygiene requirements that MUST be adhered to. **(Private03) (Did not answer)**
- i. Multifactor authentication for access to systems ii. System patches and upgrades especially for Legacy systems iii. Malware detection and response system - Automated; can explore AI tools and agents iv. SIEM tools to monitor systems and networks v. Capacity building on the usage of the tools v. (Gen Gov13) (Yes)

## Inject 4.8 – RESPONSIBLE STATE BEHAVIOUR

What would be the best strategy to deal with a non-likeminded country in ensuring responsible state behaviour?

### 1) Level of Cyber Response

- None: Do nothing in this area
- Moderate: Targeted defensive actions, cybersecurity alerts to international bodies
- High: Disruption of critical systems (e.g., cyber-attacks), cyber retaliation
- Maximum: Full-scale cyber warfare response targeting strategic infrastructure

### 2) Level of Kinetic Response

- None: Do nothing in this area
- Moderate: Military posture shift (e.g., joint exercises, no-fly zones)
- High: Limited military strikes on non-critical targets to disrupt adversary capabilities
- Maximum: Full military engagement in response to sustained cyber or hybrid attacks

### 3) Level of Attribution

- None: Do nothing in this area
- Moderate: Formal attribution via international bodies (e.g. RASO)
- High: Official attribution with evidence, public sanctions imposed
- Maximum: Immediate military or diplomatic actions based on verified attribution (direct state-to-state accusation)

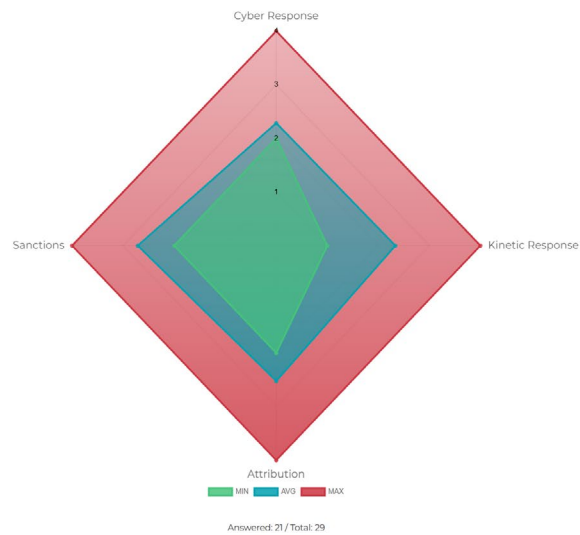
### 4) Level of Sanctions

- None: Do nothing in this area
- Moderate: Economic sanctions, suspension from international organizations (e.g. UE)
- High: Suspension of all trade relations, targeted sectoral or industry-wide sanctions
- Maximum: Comprehensive sanctions, expulsion from trade blocs, freezing bilateral cooperation agreements

All

#### 4.8 - RESPONSIBLE STATE BEHAVIOUR

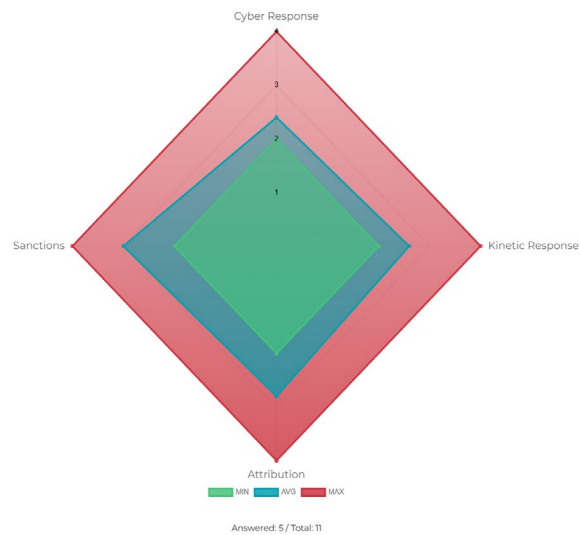
What would be the best strategy to deal with a non-likeminded country in ensuring responsible state behaviour?



WGI: Cybersecurity Governance

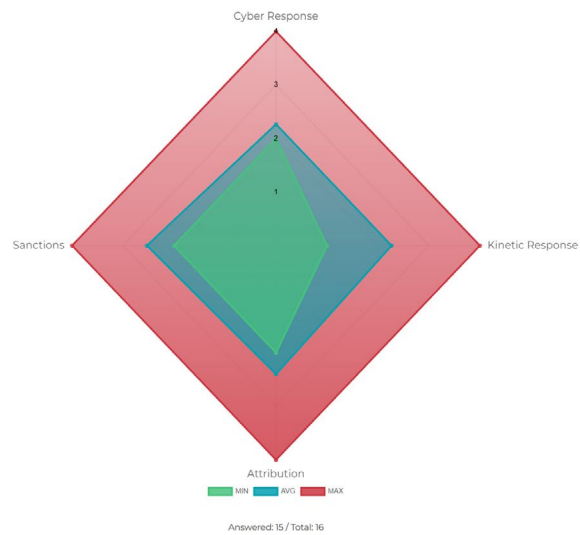
#### 4.8 - RESPONSIBLE STATE BEHAVIOUR

What would be the best strategy to deal with a non-likeminded country in ensuring responsible state behaviour?



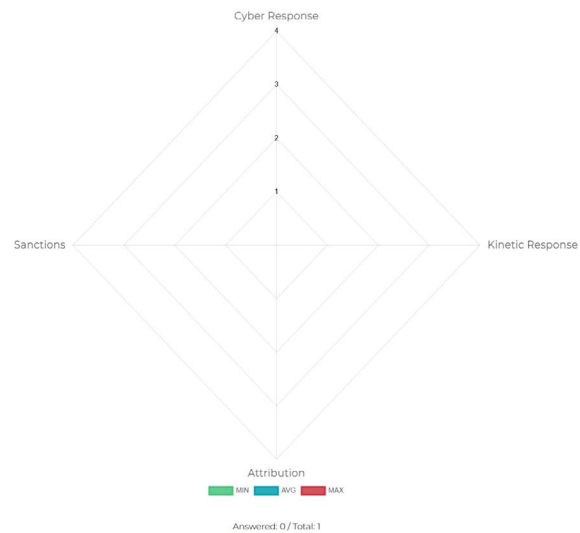
## 4.8 - RESPONSIBLE STATE BEHAVIOUR

What would be the best strategy to deal with a non-likeminded country in ensuring responsible state behaviour?



## 4.8 - RESPONSIBLE STATE BEHAVIOUR

What would be the best strategy to deal with a non-likeminded country in ensuring responsible state behaviour?



## 4.8 - RESPONSIBLE STATE BEHAVIOUR

What would be the best strategy to deal with a non-likeminded country in ensuring responsible state behaviour?

