Research report for external body :
Macdonald, S., Jarvis, L., Lavis, S. & Nouri, L. (2018). *Cyberterrorism: A Survey of Researchers Five Years On.*

Cyberterrorism:

A Survey of Researchers Five Years On

Final Report

July 2018

the
cyberterrorism
project

About the Project

The Cyberterrorism Project is an international, interdisciplinary research network that was established by academics working across a number of fields including Engineering, Law and Politics in 2011. The project has four primary objectives:

1. To further understanding amongst the scientific community by engaging in original research on the concept, threat and possible responses to terrorist uses of the internet.

2. To facilitate global networking activities around this research theme.

3. To engage with policymakers, opinion formers, citizens and other stakeholders at all stages of the research process, from data collection to dissemination.

4. To do the above within a multidisciplinary and pluralist context that draws on expertise from the physical and social sciences.

Recent activities of the Cyberterrorism Project include hosting an international Terrorism and Social Media conference in Swansea (UK), constructing a database of international definitions of cyberterrorism and conducting a study of media constructions of cyberterrorism. Findings from these activities have been published in top international journals including *Terrorism and Political Violence*, *Studies in Conflict and Terrorism*, *Perspectives on Terrorism*, and, *Journal of Terrorism Research*, and in books including *Cyberterrorism: Understanding, Assessment and Response* (Springer, 2014), *Terrorism Online: Politics, Law and Technology* (Routledge, 2015), *Violent Extremism Online: New Perspectives on Terrorism and the Internet* (Routledge, 2016) and most recently, *Terrorists' Use of the Internet: Assessment and Response* (IOS Press, 2017). Further information on the project, its members, and ongoing research activities is available via the project website: www.cyberterrorism-project.org.

For membership and media enquiries, please see the contact details on page 21.

Acknowledgements

We would like to thank all of the respondents for taking the time to complete the survey. Thanks also to Kimberly Corderoy and Conor Burns for excellent research assistance.

Suggested Citation

Macdonald, S., Lavis, S. M., Jarvis, L., & Nouri, L. (2018). *Cyberterrorism: A Survey of Researchers Five Years On*. Cyberterrorism Project Research Report (No. 8). Available via: www.cyberterrorism-project.org

About the Survey

In 2012 members of the Cyberterrorism Project conducted a survey of researchers on cyberterrorism. A total of 118 responses were received, from researchers working in 24 countries across six continents. The findings were published in a report and series of four journal articles, listed below, examining understandings of cyberterrorism, assessments of the threat it poses, whether it can be perpetrated by states and the wider cyber lexicon:

- Macdonald, S., Jarvis, L., Chen, T., & Lavis, S. M. (2013). *Cyberterrorism: A Survey of Researchers*. Cyberterrorism Project Research Report (No. 1), Swansea University (link).
- Jarvis, L., & Macdonald, S. (2015). *What is Cyberterrorism? Findings from a Survey of Researchers*. "Terrorism and Political Violence", 27(4), 657-678. doi: 10.1080/09546553.2013.847827.
- Jarvis, L., Macdonald, S. & Nouri, L. (2014). *The Cyberterrorism Threat: Findings from a Survey of Researchers*. "Studies in Conflict & Terrorism", 37(1), 68-90. doi: 10.1080/1057610X.2014.853603.
- Macdonald, S., Jarvis, L., & Nouri, L. (2015). State Cyberterrorism: A Contradiction in Terms? Journal of Terrorism Research, 6(3), 62-75. doi: 10.15664/jtr.1162.
- Jarvis, L., & Macdonald, S. (2014). *Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon*. "Perspectives on Terrorism", 8(2), 52-65 (link).

Members of the project team also presented the findings to numerous non-academic stakeholders, including NATO COE-DAT, UNICRI, and the European Defence Agency.

In 2017 we ran the survey again – "five years on" – to investigate how opinions had changed (if at all): 12 questions remained the same as the 2012 survey; two questions were reformulated; and four new questions were posed.

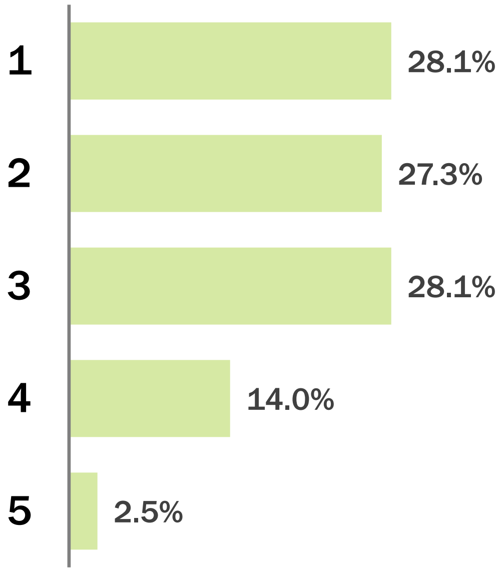
A total of 120 complete responses and four partial responses were received, from researchers working in 30 countries across five continents. This report summarizes our initial findings.

Table of Contents

To what extent have the definitional issues around terrorism in general been satisfactorily resolved? (where 1 = not at all and 5 = entirely)

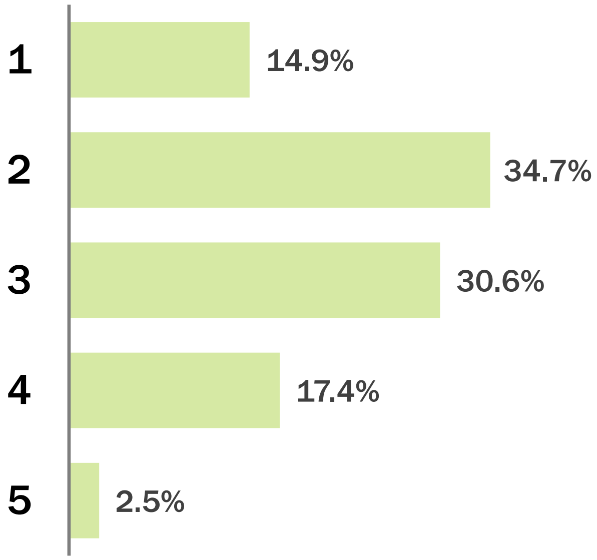
	Not at all 1	2	3	4	Entirely 5
For policymakers? (*n* = 121; response rate = 97.6%)	34	33	34	17	3
For researchers? (*n* = 121; response rate = 97.6%)	18	42	37	21	3

For policymakers:



25th Percentile	1
Median	2
75th Percentile	3
Mean	2.355
Std. Dev.	1.110

For researchers:

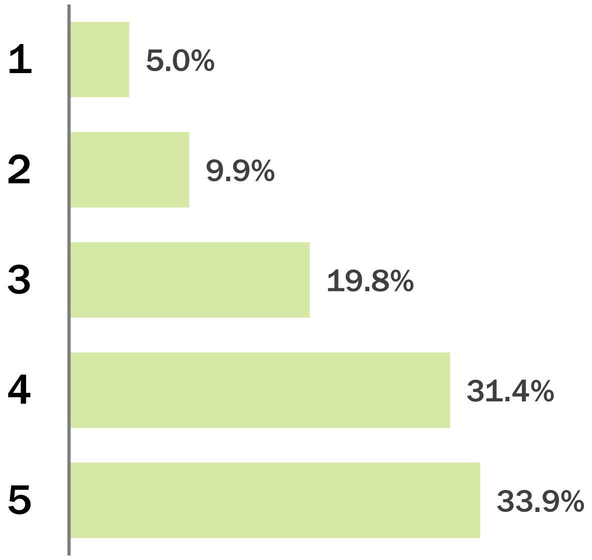


25th Percentile	2
Median	3
75th Percentile	3
Mean	2.579
Std. Dev.	1.023

How important is, or was, the resolution of the definitional issues around terrorism? (where 1 = not at all and 5 = very important)

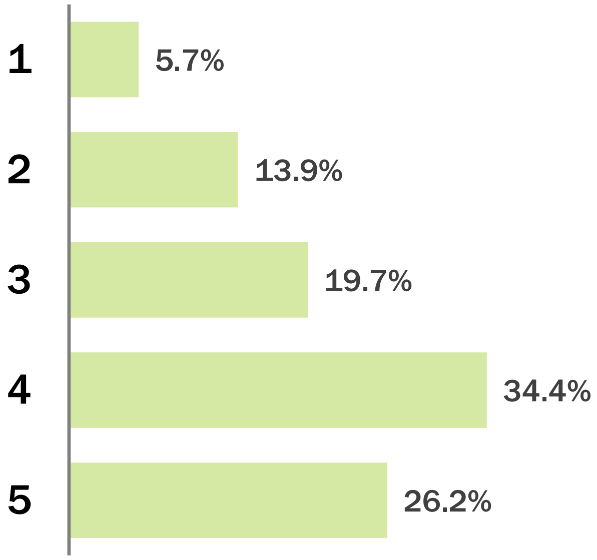
	Not at all 1	2	3	4	Very important 5
For policymakers? (*n* = 121; response rate = 97.6%)	6	12	24	38	41
For researchers? (*n* = 122; response rate = 98.4%)	7	17	24	42	32

For policymakers:



25th Percentile	3
Median	4
75th Percentile	5
Mean	3.793
Std. Dev.	1.161

For researchers:

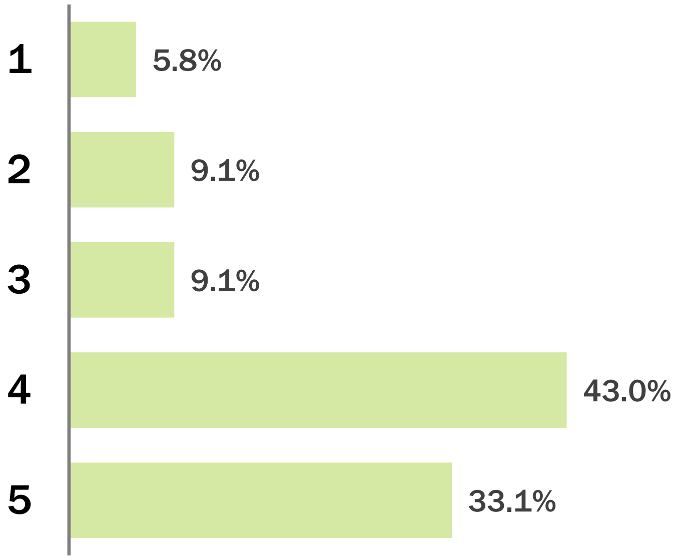


25th Percentile	3
Median	4
75th Percentile	5
Mean	3.615
Std. Dev.	1.181

How necessary do you believe a specific definition of cyberterrorism to be? (where 1 = of no use and 5 = essential)

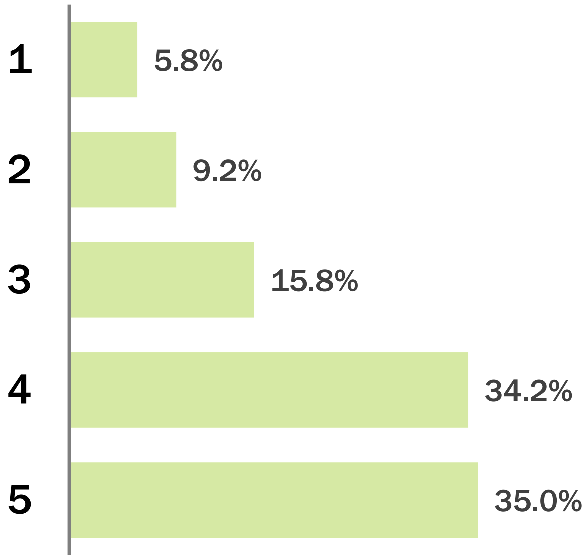
	Of no use 1	2	3	4	Essential 5
For policymakers? (*n* = 121; response rate = 97.6%)	7	11	11	52	40
For researchers? (*n* = 120; response rate = 96.8%)	7	11	19	41	42

For policymakers:



25th Percentile	4
Median	4
75th Percentile	5
Mean	3.884
Std. Dev.	1.142

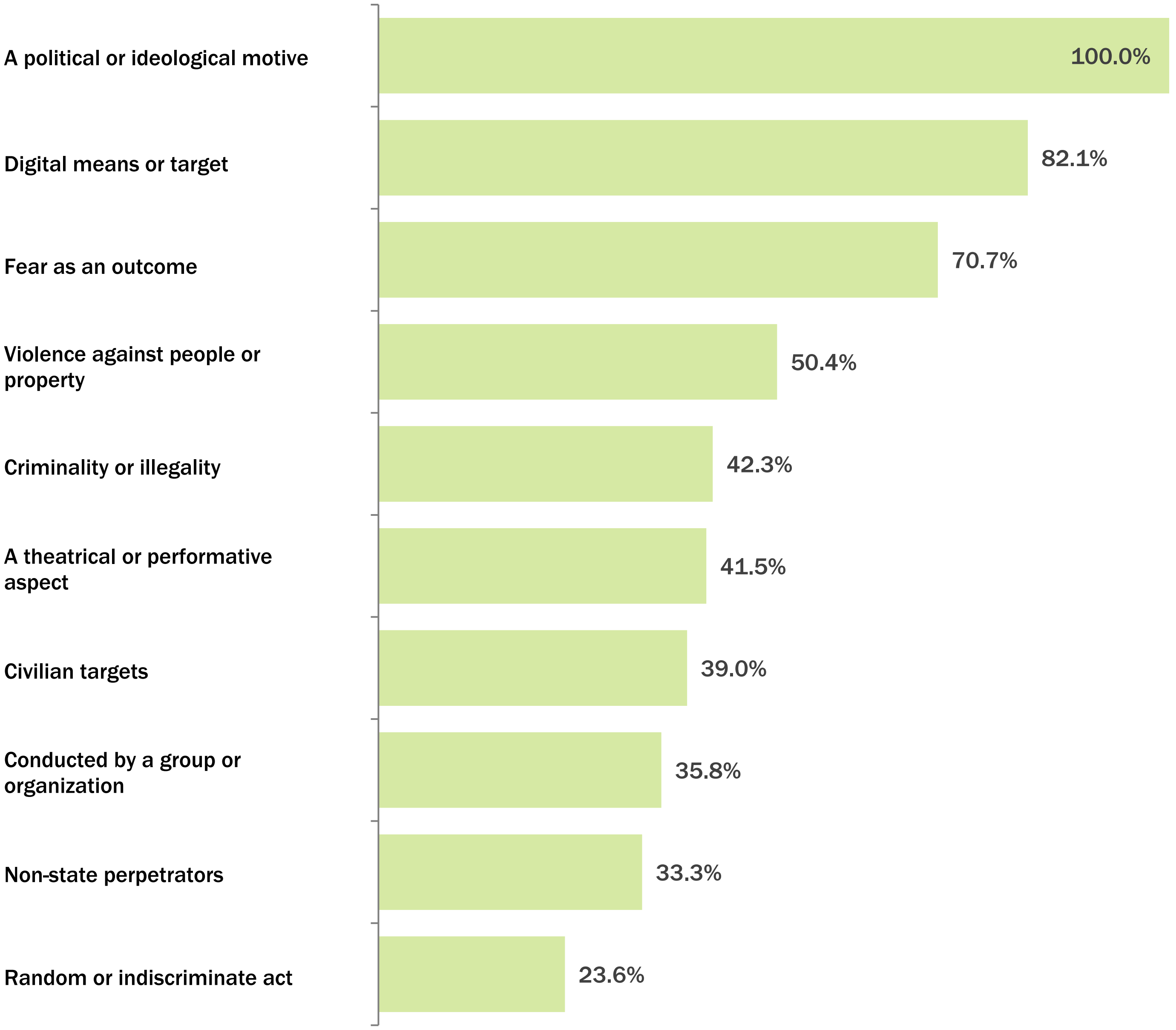
For researchers:



25th Percentile	3
Median	4
75th Percentile	5
Mean	3.833
Std. Dev.	1.176

In your view, which of the following are important elements of cyberterrorism?

123 individuals responded to this question (response rate: 99.2%). One respondent chose not to engage, citing an epistemological objection to the question.



In your view, are any important elements of cyberterrorism missing from this list?

A total of 48 respondents answered here (response rate: 38.7%). Some listed more than one element.

Targets critical infrastructure: 8 respondents

Example: “Mass or targeted service disruption that threatens life or wellbeing, e.g. to water supply, electricity, aviation, health services for political or ideological motives” (R7066)

State sponsored, supported or perpetrated: 8 respondents

Example: “Cyberterrorism, like its analogue parent, can be carried out as much by state as non-state actors” (R7107)

Intention to coerce or compel a target audience: 4 respondents

Example: “Attack is not only directed against the actual victim(s) but against a wider target group (audience) whom the perpetrator(s) intend(s) to coerce/intimidate” (R7064)

Other targets, e.g. government, military, economic and financial targets: 3 respondents

Example: “Targets that are non-civilian such as police, first responders and governmental employees” (R7074)

Propagandising: 2 respondents

Example: “Propaganda that serves to radicalise, recruit or encourage violence or the threat of violence” (R7088)

Creates doubt, insecurity or loss of confidence: 2 respondents

Example: “Other outcomes besides fear include anxiety, stress, insecurity, political polarization, loss of confidence and dysfunction at the level of social discourse” (R7116)

Secrecy: 2 respondents

Example: “Veiled origins of attack” (R7079)

Responses from just one respondent included:

- Hate (R7006)
- Revenge (R7006)
- Provocation (R7046)
- Group identity (R7051)
- Targets personal data (R7110)

In which of the following scenarios do the actions of a terrorist group constitute cyberterrorism (if any)?

The majority of scenarios posed were answered by all respondents (response rate: 100%); one individual did not respond to scenario 3 (response rate for scenario 3: 99.2%).

Scenario 1: A terrorist group interferes with an air traffic control system, causing two passenger aircraft to collide in mid-air

Constitutes cyberterrorism: 101 respondents (81.5%) Don't know: 15 respondents (12.1%)
Does not constitute cyberterrorism: 8 respondents (6.5%)

Scenario 2: Tensions between two communities boil over, resulting in violent rioting. Several people are killed. A terrorist group seeks to further inflame the situation. Posing as members of one of the communities, they post gruesome images and videos on social media and issue threats against members of the other community

Constitutes cyberterrorism: 37 respondents (29.8%) Don't know: 11 respondents (8.9%)
Does not constitute cyberterrorism: 76 respondents (61.3%)

Scenario 3: A terrorist group remotely accesses the processing control systems of a cereal manufacturer and changes the levels of iron supplement. As a result large numbers of children fall ill, and some die

Constitutes cyberterrorism: 100 respondents (81.3%) Don't know: 11 respondents (8.9%)
Does not constitute cyberterrorism: 12 respondents (9.8%)

Scenario 4: A terrorist group hacks the computer system of the nation's stock exchange, sending the national economy into chaos and causing significant economic damage

Constitutes cyberterrorism: 95 respondents (76.6%) Don't know: 16 respondents (12.9%)
Does not constitute cyberterrorism: 13 respondents (10.5%)

Scenario 5: A terrorist group plants a bomb in the computer control room of the nation's stock exchange. Although no-one is killed, the computers are destroyed, sending the national economy into chaos and causing significant economic damage

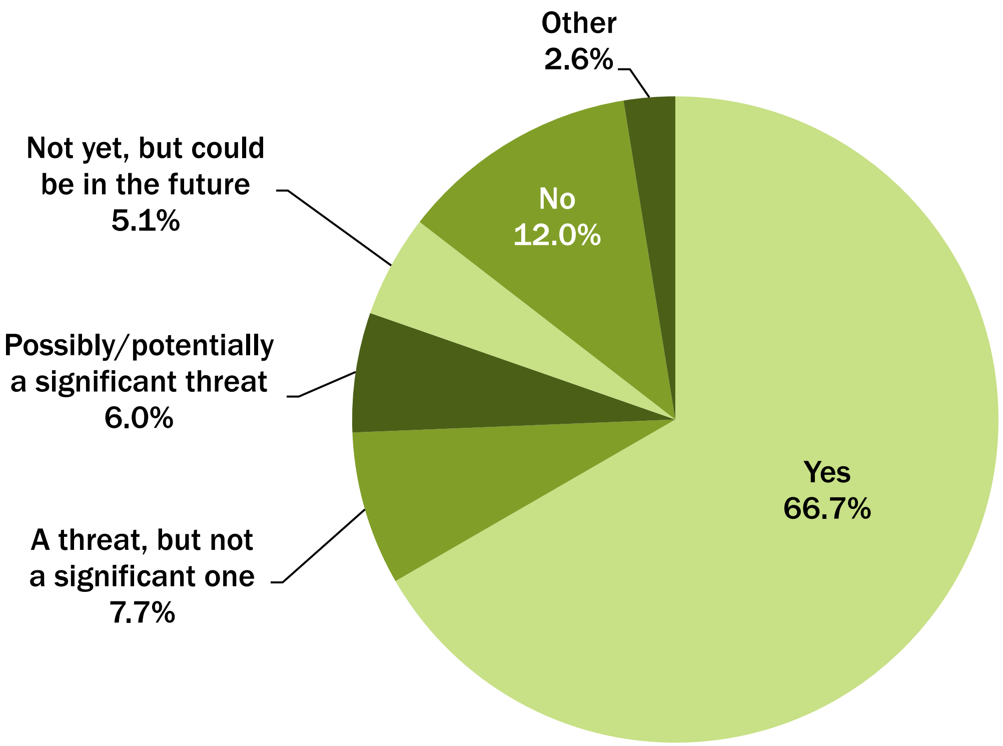
Constitutes cyberterrorism: 36 respondents (29.0%) Don't know: 9 respondents (7.3%)
Does not constitute cyberterrorism: 79 respondents (63.7%)

Scenario 6: A terrorist group plans to hijack a plane and crash it into a busy urban area. They buy their flight tickets online

Constitutes cyberterrorism: 8 respondents (6.5%) Don't know: 4 respondents (3.2%)
Does not constitute cyberterrorism: 112 respondents (90.3%)

In your view, does cyberterrorism constitute a significant threat? If so, against whom or what is the threat focused?

117 respondents answered the first part of this question (response rate: 94.4%).



The three "other" responses were each equivocal, in different respects:

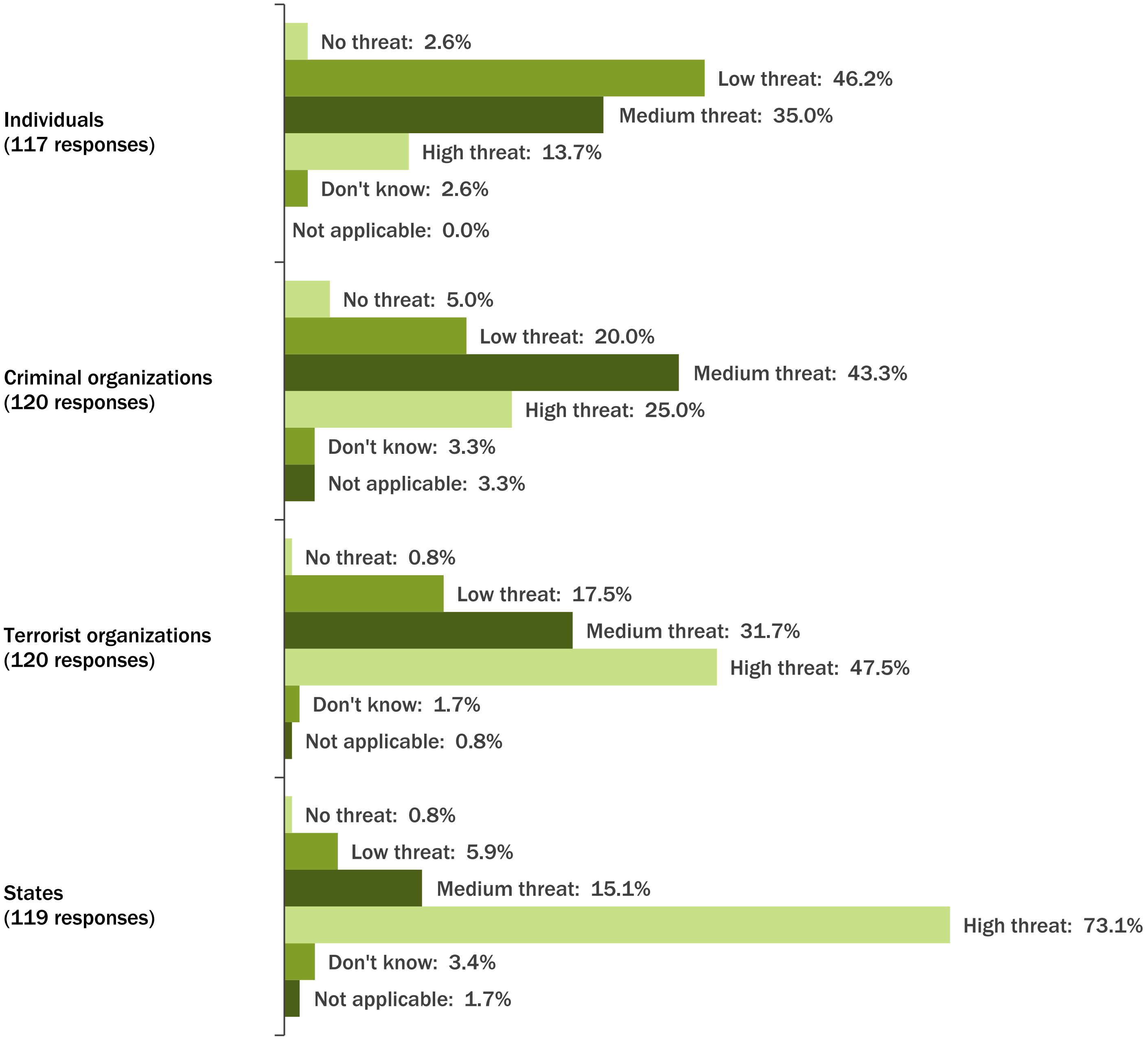
- One said it would depend on what "threat" means (R7003)
- One said it would depend on what "significant" means (R7078)
- The other simply said: "Depends" (R7101)

92 respondents (response rate: 74.2%) answered the second part of the question. The following were identified as referents of the threat (some respondents listed more than one of these):

- Governments/states: 28 respondents
- Critical infrastructures/computer networks: 26 respondents
- Civilians/individuals: 26 respondents
- Organisations/private sector/economy/corporations: 19 respondents
- Society/societies: 8 respondents
- Anyone/everyone; anywhere/everywhere: 8 respondents
- The West: 6 respondents
- Groups: 3 respondents
- Elections/electoral systems: 3 respondents
- The United States: 3 respondents
- Cultures/ethnic groups: 2 respondents
- Military: 2 respondents

What, in your opinion, is the cyberterrorism threat level posed by each of the following actors?

Participation in this question varied by actor: the number of responses received is indicated in the axis.



Respondents were also asked to identify any other actors not represented in the question. 59 respondents (response rate: 47.9%) answered. The following actors were identified as potential threats:

- “Groups” or “networks” of individuals: 5 respondents
- Hacktivists: 4 respondents
- Unknown actors who cannot be identified pre-emptively: 3 respondents
- Proxies operating on behalf of another target: 3 respondents
- Members of business/private sector: 2 respondents
- The group “Anonymous”: 2 respondents

Five other respondents did not name specific actors, commenting on the difficulty or futility of attempting to do so given the nature of cyberterrorism.

From where in the world is cyberterrorism most likely to emerge?

103 respondents (response rate: 83.0%) provided a response to this question. Responses were categorized into five groups: specific locations; broad geographic regions; state-related descriptors; party or identity-based classifications; and non-geographic or participant-specific classifications.

Specific locations:

Russia	31 (25.0%)	Israel	3 (2.4%)	Nepal	1 (0.8%)
China	16 (12.9%)	Iran	1 (0.8%)	Pakistan	1 (0.8%)
North Korea	8 (6.5%)	Korea (singular)	1 (0.8%)	Saudi Arabia	1 (0.8%)
United States	6 (4.8%)	Mongolia	1 (0.8%)	United Kingdom	1 (0.8%)

Broad geographic locations/regions

Anywhere/ everywhere	27 (21.8%)	Soviet Union or Eastern Europe	4 (3.2%)	Africa	1 (0.8%)
The Middle East	13 (10.5%)	The West	4 (3.2%)	Europe	1 (0.8%)
Asia	4 (3.2%)	An “Arab” location	2 (1.6%)	The Maghreb region	1 (0.8%)

State-related descriptors

“States” (no further qualification)	7 (5.7%)	“Rogue states”	2 (1.6%)	“State-related”	1 (0.8%)
“Non-state”	2 (1.6%)	“State-supported”	2 (1.6%)	“States with terrorism”	1 (0.8%)

Party or identity-based classifications

Terrorist/s	5 (4.0%)	Islam/Islamic	3 (2.4%)	Intelligence agencies	2 (1.6%)
ISIS	3 (2.4%)	Al-Qaeda	2 (1.6%)	Hackers	1 (0.8%)

Non-geographic or participant-specific classifications

“Developed” places	3 (2.4%)	The “ether”	1 (0.8%)	The Third World	1 (0.8%)
“Developing” places	3 (2.4%)	The First World	1 (0.8%)	The “Underworld”	1 (0.8%)
Places facing “conflict”	2 (1.6%)				

Where in the world is most vulnerable to cyberterrorism?

99 respondents (response rate: 79.8%) provided a response to this question. Responses were categorized using the same framework as the previous question. However, there were no references to actors as target, meaning the previous "party or identity-based classifications" group was unpopulated.

Specific locations:

United States	20 (16.1%)	United Kingdom	2 (1.6%)	Iran	1 (0.8%)
China	3 (2.4%)	Australia	1 (0.8%)	Namibia	1 (0.8%)
Russia	3 (2.4%)	Estonia	1 (0.8%)	North Korea	1 (0.8%)
Canada	2 (1.6%)	France	1 (0.8%)	South Korea	1 (0.8%)
Japan	2 (1.6%)				

Broad geographic locations/regions

The West/Western countries	11 (21.8%)	Western Europe	5 (4.0%)	The "Global South"	1 (0.8%)
Anywhere/ everywhere	10 (21.8%)	North America	3 (2.4%)	The Middle East	1 (0.8%)
Europe/the EU	9 (3.2%)	The "Global North"	1 (0.8%)		

State-related descriptors

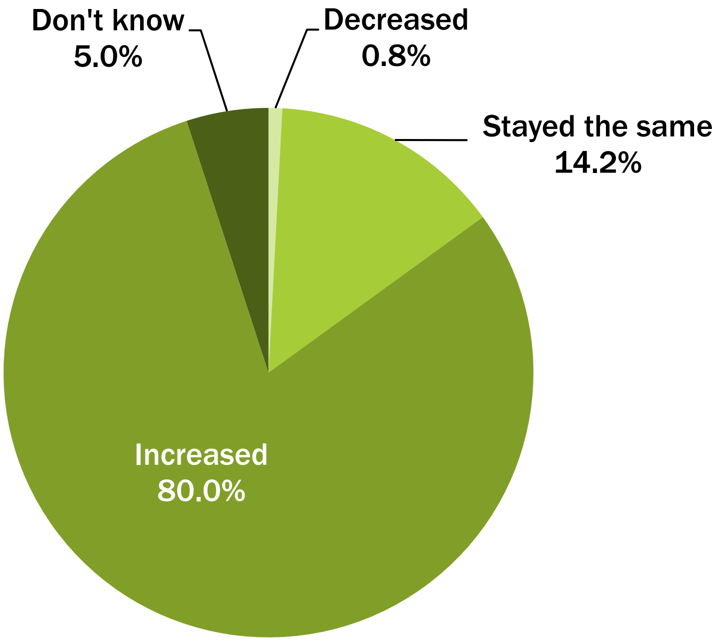
References to "state/s" indicating a "positive" development status	4 (3.2%)	"States", without further qualification	1 (0.8%)
References to "state/s" indicating a "negative" development status	3 (2.4%)		

Non-geographic or participant-specific classifications

"Developed" places	11 (8.9%)	References "cyber"	4 (3.2%)	References "networks"	3 (2.4%)
"Dependent" places	8 (6.5%)	Includes "society/ies"	4 (3.2%)	Democracies	2 (1.6%)
"Reliant" on networks	6 (4.8%)	References "technology"	4 (3.2%)	The Third World	2 (1.6%)
"Connected" places	5 (4.0%)	Includes "advanced"	3 (2.4%)	The First World	1 (0.8%)
"Developing" places	5 (4.0%)	References "economy"	3 (2.4%)		

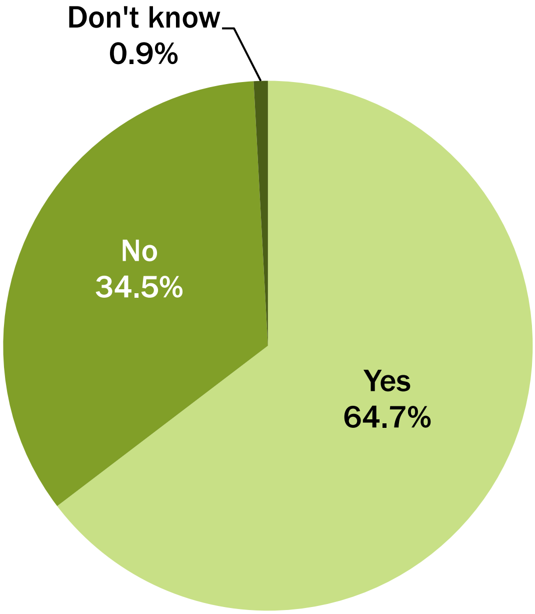
In your opinion, has the cyberterrorism threat level changed in the last five years?

120 respondents answered this question (response rate: 96.8%).



With reference to your previous responses, do you consider that a cyberterrorist attack has ever taken place? Please explain.

116 individuals answered this question (response rate: 93.6%).



A total of 26 different incidents were identified as examples of cyberterrorism. Of these, the most frequently cited were:

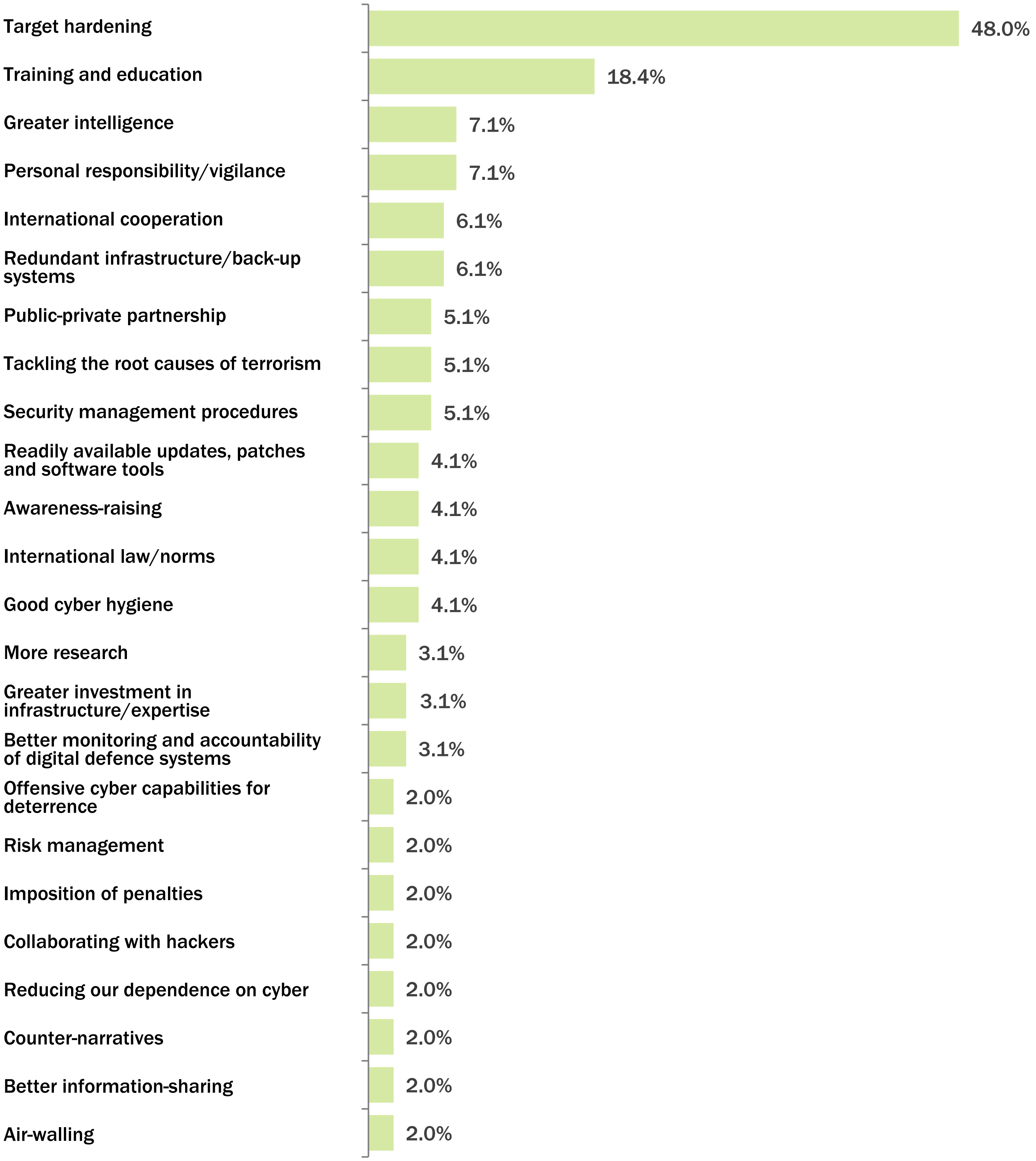
- Stuxnet: 8 respondents
- Attacks on Ukraine: 5 respondents
- WannaCry ransomware: 5 respondents
- Attacks on Estonia: 4 respondents
- Interference in the 2016 US Presidential election: 3 respondents
- Petya ransomware: 2 respondents
- Attack on TV5Monde: 2 respondents

Those that answered “no” provided a number of explanations, including:

- Cyberattacks to date have been committed by perpetrators lacking a political motive and/or the intention to create terror: 6 respondents
- Cyberattacks to date have not resulted in violence against people or property: 5 respondents
- Cyberattacks to date have not been severe enough to qualify as cyberterrorism: 4 respondents
- Cyberattacks to date have not been perpetrated by non-state actors: 3 respondents

In your view, what are the most effective countermeasures against cyberterrorism?

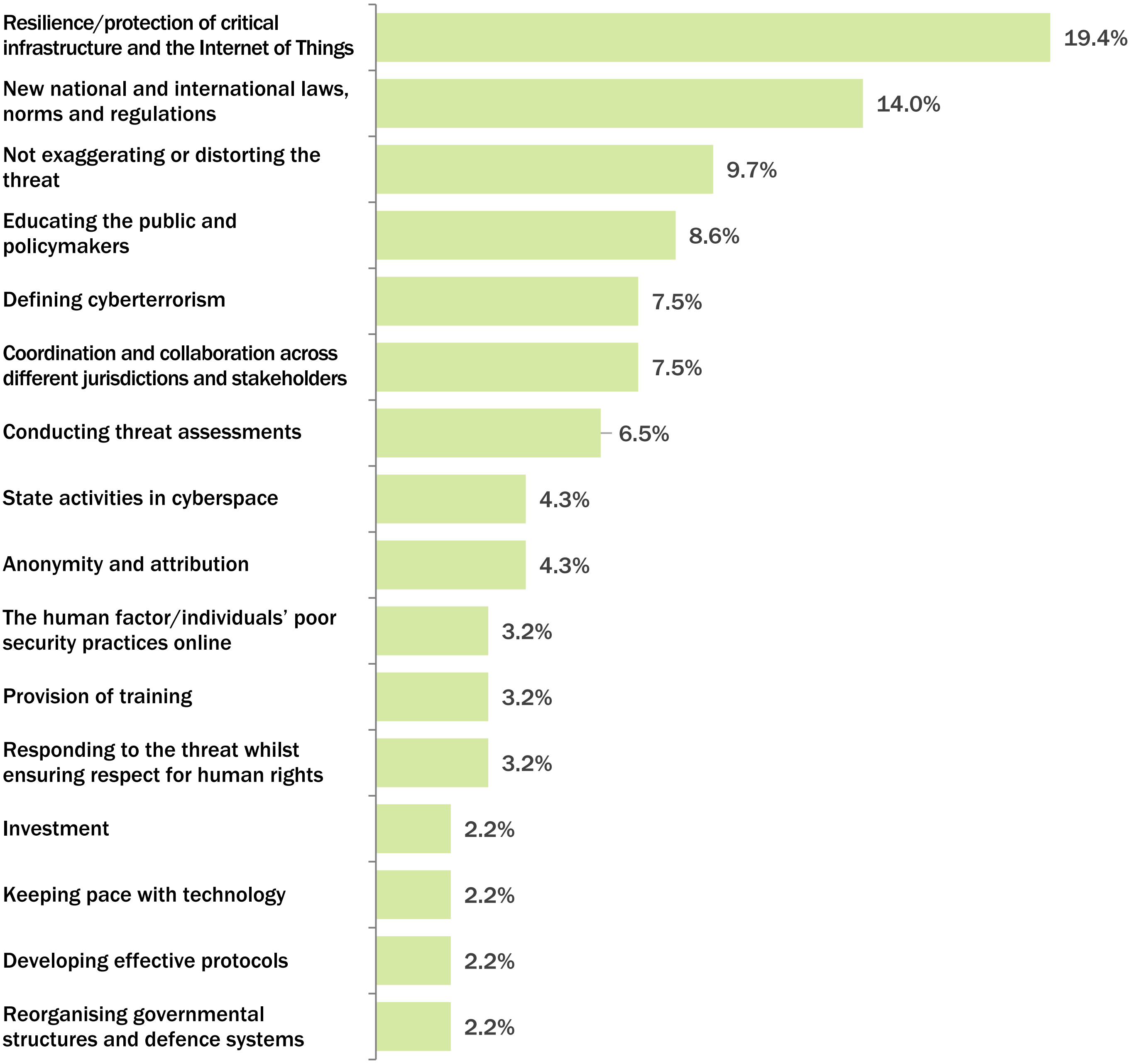
98 individuals answered this question (response rate: 79.0%). The following 24 countermeasures were all identified by two or more respondents:



Six respondents said they did not know, or were unsure, which countermeasures would be most effective. This was primarily due to lack of relevant expertise.

What are the most pressing issues in the realm of cyberterrorism for policymakers?

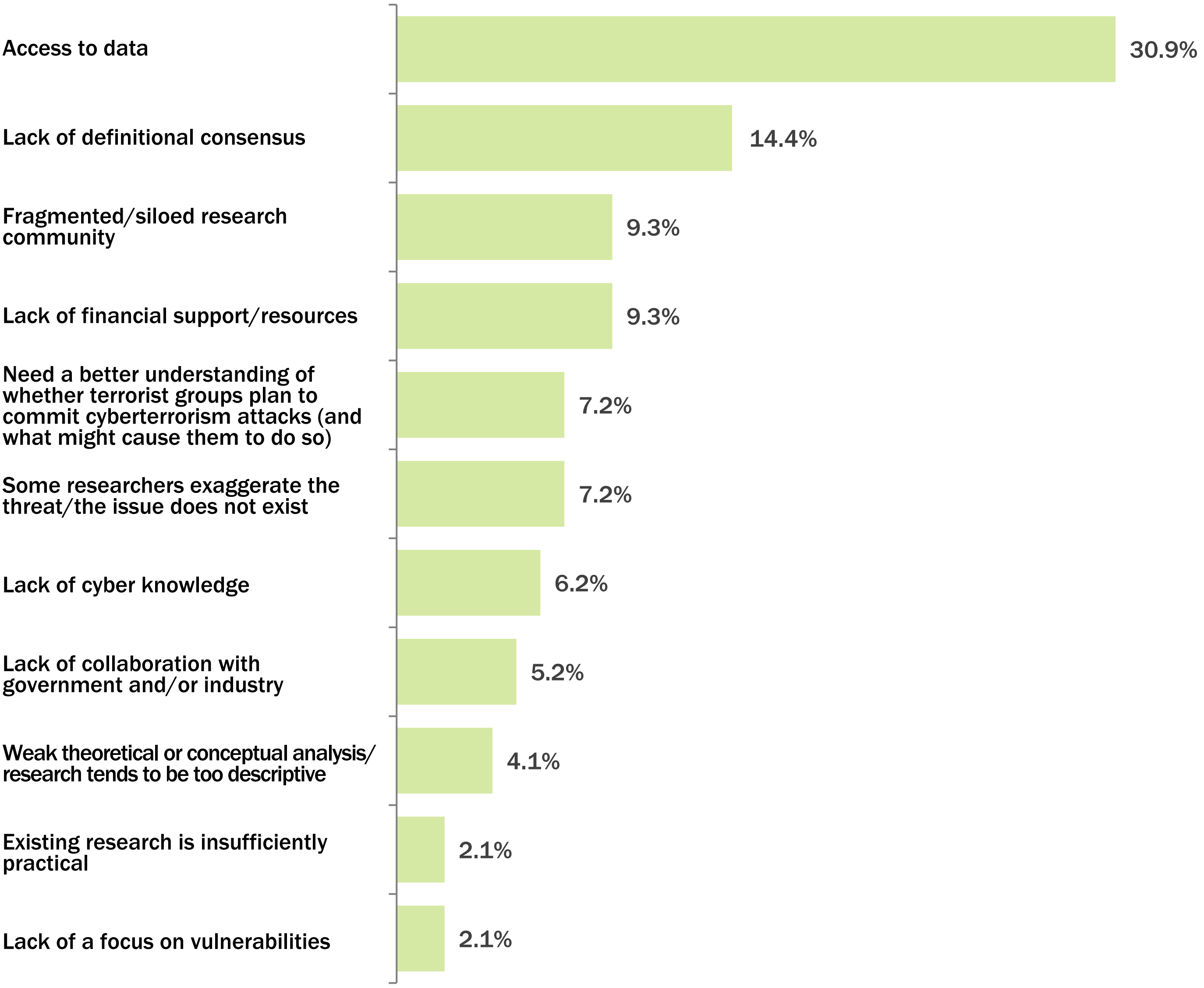
93 individuals answered this question (response rate: 75.0%). The following 16 issues were all identified by two or more respondents:



Three respondents said they did not know what are the most pressing issues facing policymakers.

What are the major limitations, gaps, or weaknesses within academic research into cyberterrorism?

97 individuals answered this question (response rate: 78.2%). The following 11 issues were all identified by two or more respondents:



Six respondents said they didn’t know or weren’t sure of the most pressing issues facing researchers.

In which country is your place of employment?

In addition to the 117 responses summarized below, 7 respondents (5.6% of total respondents) did not answer this question.

United States	43 (34.7%)	The Netherlands	2 (1.6%)	Nigeria	1 (0.8%)
United Kingdom	21 (16.9%)	Slovenia	2 (1.6%)	Norway	1 (0.8%)
Australia	8 (6.5%)	Turkey	2 (1.6%)	Poland	1 (0.8%)
Canada	6 (4.8%)	Ukraine	2 (1.6%)	Romania	1 (0.8%)
Belgium	3 (2.4%)	Austria	1 (0.8%)	Russia	1 (0.8%)
Czech Republic	3 (2.4%)	Denmark	1 (0.8%)	South Africa	1 (0.8%)
Germany	3 (2.4%)	Greece	1 (0.8%)	Spain	1 (0.8%)
Israel	2 (1.6%)	Ireland	1 (0.8%)	Sweden	1 (0.8%)
Italy	2 (1.6%)	Kuwait	1 (0.8%)	Switzerland	1 (0.8%)
Malaysia	2 (1.6%)	New Zealand	1 (0.8%)	United Arab Emirates	1 (0.8%)

How would you classify your current employment?

Respondents gave an open-ended response to this question. In addition to the 116 responses summarized, 8 respondents (6.5%) declined to answer.

Academic staff	89 (71.8%)	Retired	3 (2.4%)
Independent researcher	15 (12.1%)	None of the above	4 (3.2%)
Research student	5 (4.0%)		

How would you classify your primary disciplinary background?

Respondents gave an open-ended response to this question. In addition to the 116 responses summarized, 8 respondents (6.5%) declined to answer.

Group A:	Political Science, International Relations, et al.	52 (46.0%)
Group B:	Law, Criminology, et al.	15 (13.3%)
Group C:	Economics, Business, et al.	1 (0.9%)
Group D:	Engineering, Computer Science, Cyber, et al.	18 (15.9%)
Group E:	Psychology, Anthropology, et al.	15 (13.3%)
Group F:	Literature, Arts, History, et al.	6 (5.3%)
Participants who responded but could not be classified into these groups		6 (5.3%)

the
cyberterrorism
project

Corresponding Author Contact Information

Prof. Stuart Macdonald
College of Law & Criminology
Swansea University

s.macdonald@swansea.ac.uk
@CTProject_SM

Project Contact Information

ctproject@swansea.ac.uk

www.cyberterrorism-project.org

www.facebook.com/CyberterrorismProject

@CTP_Swansea