Cyberterrorism:
A Survey of Researchers

March 2013

the
cyberterrorism
project

About the Survey

This report provides an overview of findings from a project designed to capture current understandings of cyberterrorism within the research community. The project ran between June and November 2012, and employed a questionnaire which was distributed to over 600 researchers, authors and other experts. Potential respondents were identified using a combination of methods, including targeted literature reviews, standing within relevant academic communities, snowballing from earlier participants or contacts, and the use of two mailing lists. 118 responses were received in total, from individuals working in 24 countries across six continents. Please contact the research team with any enquiries on the project's methods and findings (see p. 21 for contact details).

About the Project

The Cyberterrorism Project was established at Swansea University, UK in 2011 by academics working in the School of Law, College of Engineering, and Department of Political and Cultural Studies. The project has the following objectives:

(1) To further understanding amongst the scientific community by engaging in original research on the concept, threat and possible responses to cyberterrorism.
(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.

Further information on the project, its members, and current research activities is available via the project website: www.cyberterrorism-project.org

Acknowledgements

We would like to thank the Swansea Academy of Learning and Teaching and the College of Business, Economics & Law, Swansea University, for their support for this survey.

Our gratitude also goes to all of the academics and researchers who took the time to respond to this survey, and to Jo Halbert, David Mair, Lella Nouri and Andrew Whiting for their helpful suggestions.

Suggested Citation

Macdonald, S., Jarvis, L., Chen, T. & Lavis, S. (2013). *Cyberterrorism: A Survey of Researchers*. Cyberterrorism Project Research Report (No. 1), Swansea University. Available via: www.cyberterrorism-project.org

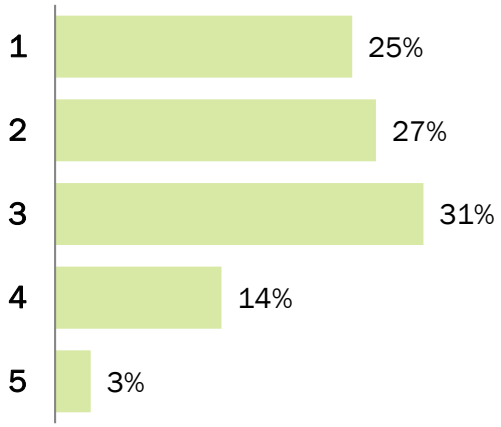
Table of Contents

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=114, response rate: 97%)	29	31	35	16	3
For researchers? (n=118, response rate: 100%)	15	25	48	26	4

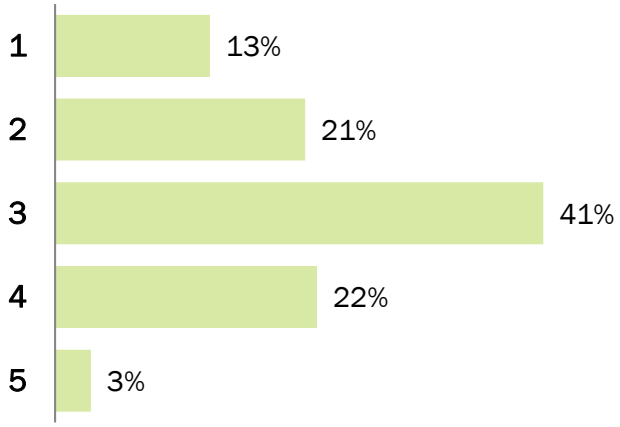
(Four respondents answered only in respect of researchers)

For policymakers



25th Percentile	1
Median	2
75th Percentile	3
Mean	2.412
Standard Deviation	1.096

For researchers



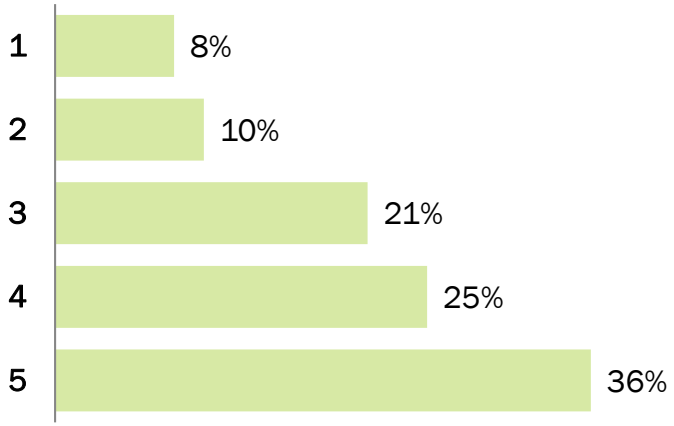
25th Percentile	2
Median	3
75th Percentile	3
Mean	2.822
Standard Deviation	1.026

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				Very important
	1	2	3	4	5
For policymakers? (n=111, response rate: 94%)	9	11	23	28	40
For researchers? (n=115, response rate: 97%)	5	18	27	32	33

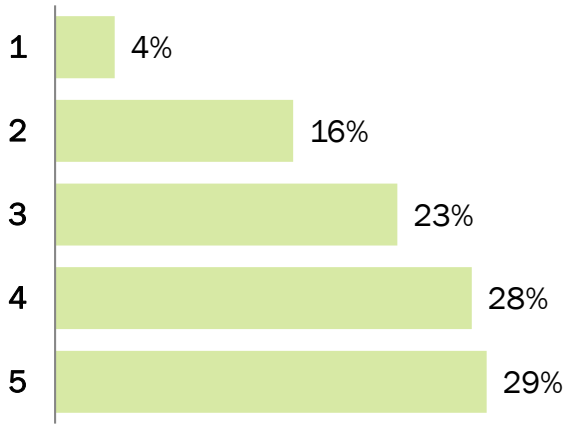
(Four respondents answered only in respect of researchers)

For policymakers



25th Percentile	3
Median	4
75th Percentile	5
Mean	3.712
Standard Deviation	1.275

For researchers



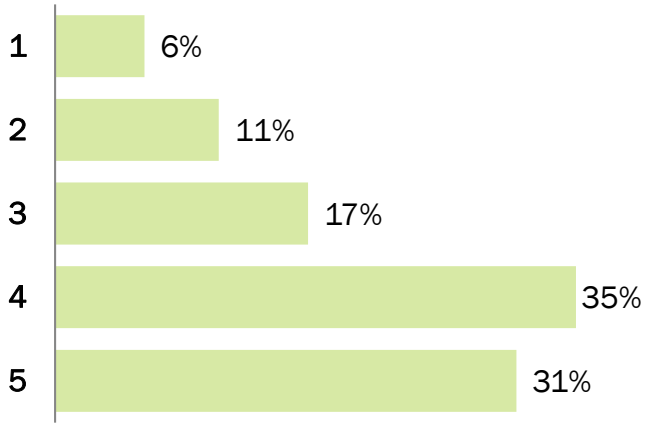
25th Percentile	3
Median	4
75th Percentile	5
Mean	3.609
Standard Deviation	1.182

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=114, response rate: 97%)	7	13	19	40	35
For researchers? (n=118, response rate: 100%)	7	20	25	38	28

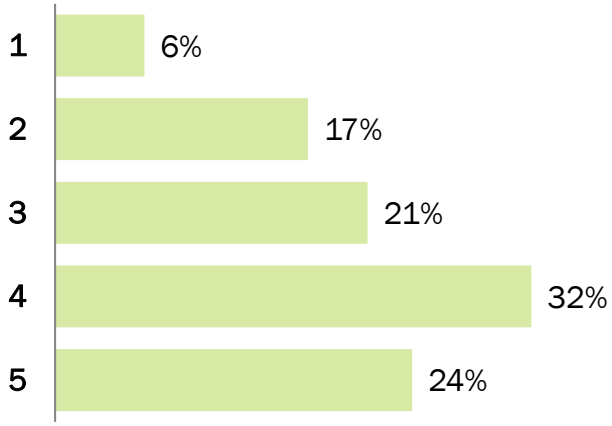
(Four respondents answered only in respect of researchers)

For policymakers



25th Percentile	3
Median	4
75th Percentile	5
Mean	3.728
Standard Deviation	1.192

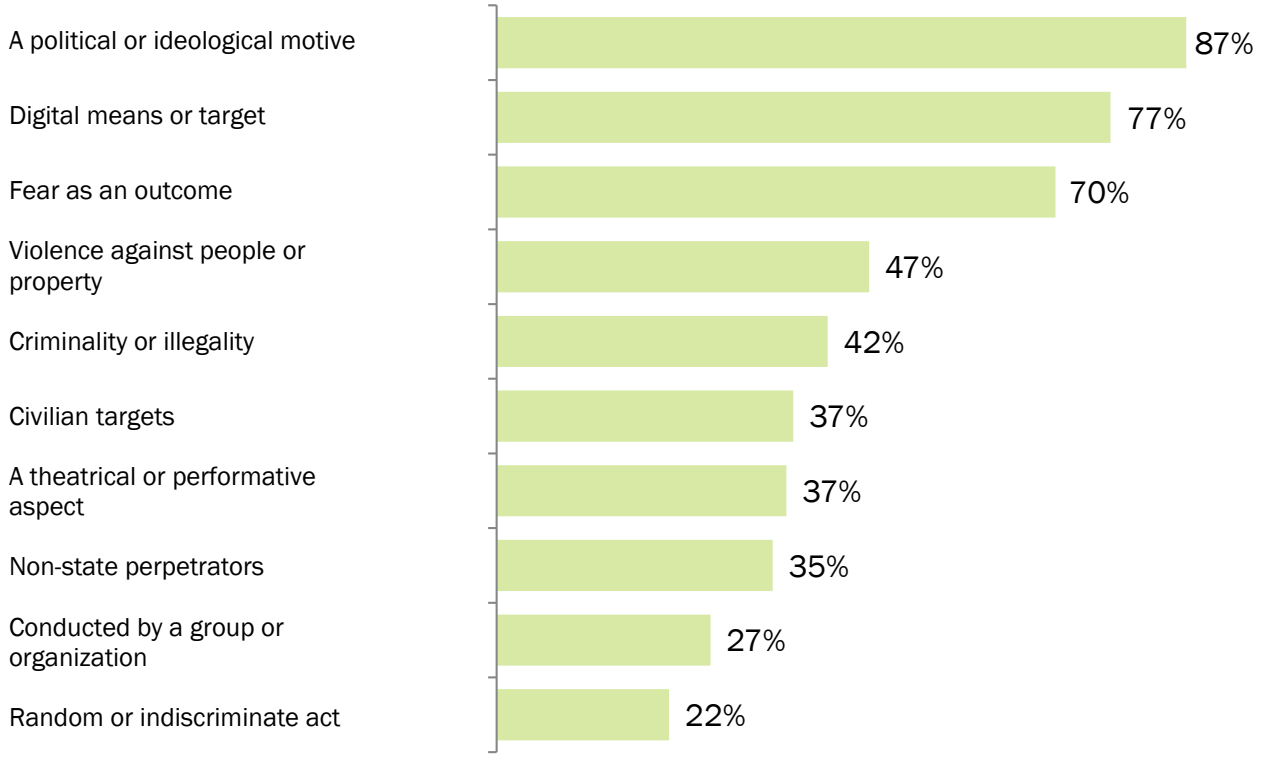
For researchers



25th Percentile	3
Median	4
75th Percentile	4
Mean	3.508
Standard Deviation	1.196

In your view, which of these are important elements of cyberterrorism?

115 individuals answered this question (response rate: 97%).



Three respondents declined to answer. Each cited similar reasons, illustrated by the following:

- "In my view the most important element of cyberterrorism is who is creating the definition and who is applying that definition to what action and to which people? In other words, it only becomes cyberterrorism after someone has labelled an action as such" – R97.

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

A total of 50 respondents answered here (response rate: 43%). Some listed more than one element.

Harm/disruption to infrastructure: 7 respondents.

Example: "It's about the disruption of ICT systems. The effects will spill over to non-digital social processes, but the immediate target is something digital" – R63.

Possibility of state perpetration: 6 respondents.

Example: "Why would state perpetrators be excluded? That's part of the propaganda view of 'terrorism', which holds that states and their agents can't be terrorists, only non-state entities can, which is a scientifically invalid distinction" – R15.

Coercion or terror in a wider audience: 6 respondents.

Example: "More than 'fear as an outcome' – cyber-enabled terrorism should – at a minimum – create terror. As a strategy this is the 'end' – everything else is a 'way' or a 'means'" – R34.

Demonstration of perpetrator skill/capability: 3 respondents.

Example: "Cyberterrorism involves a terrorist having a high level of capability. This level of capability is derived from a specific skill set: Supervisory Control and Data Acquisition Systems (SCADA); Industrial Control Systems (ICS); Information Communication Technologies (ICTs)" – R52.

Causes harm/damage: 2 respondents.

Example: "An element of damage (or a threat of damage) as a result of an attack should be included as well" – R53.

Low cost: 2 respondents.

Example: "Big media influence with small (money, time, effort) input" – R70.

Other motives:

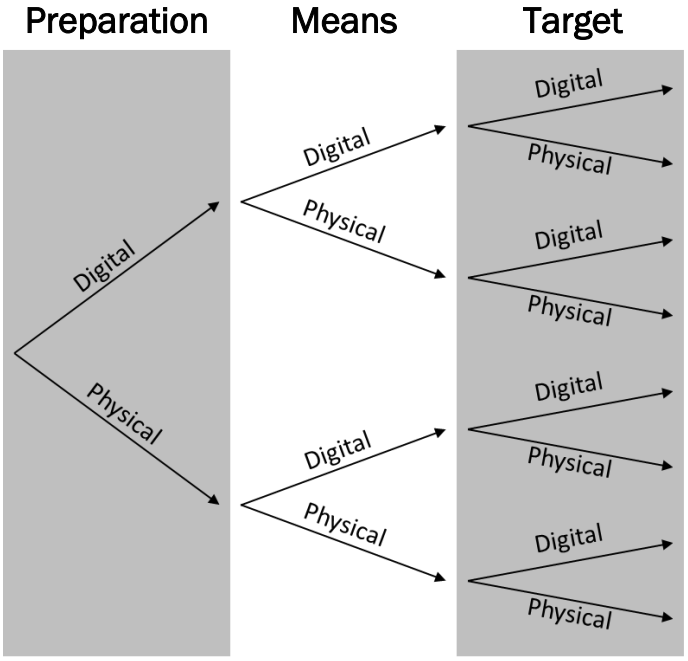
- Social or economic motives – R16.
- Religious motives – R27.

Other responses:

- Threat to national security – R82.
- Large scale – R78.
- Violation of international law – R16.
- Brainwashing – R98.
- Entertainment – R66.

In your view, which of the following scenarios constitutes an act of cyberterrorism?

This question presented eight scenarios (A-H), with each one consisting of a different combination of physical or digital preparation, means and target. Respondents were asked to select from three answers: yes; potentially; or no. 92 respondents completed this question in full (response rate: 80%). A further 13 completed it in part. The figures in the table are the percentage of respondents who responded to that scenario.



	Yes	Potentially	No
A	77%	20%	3%
B	60%	30%	10%
C	49%	24%	27%
D	20%	19%	61%
E	70%	24%	6%
F	38%	44%	18%
G	33%	36%	31%
H	9%	13%	78%

A number of respondents took the opportunity to enter comments on the diagram:

Question or diagram unclear or lacking sufficient explanation: 9 respondents.

Motive or intention is more significant than the location of an attack's preparation, means or target: 6 respondents.

Example: "Would not the key issue be intent rather than where and by whom an event was planned and executed?" – R103.

The target may be digital but the attack must result in physical violence: 4 respondents.

Example: "The question of how you define the target is very important. If a terrorist group attacks an ICT system (digital) that controls people's drinking water supply (physical), the immediate target is digital, but the goal of the attack is to harm people physically. In my view, disrupting an ICT system is rarely, if ever, a goal in itself in a cyber terrorist attack" – R63.

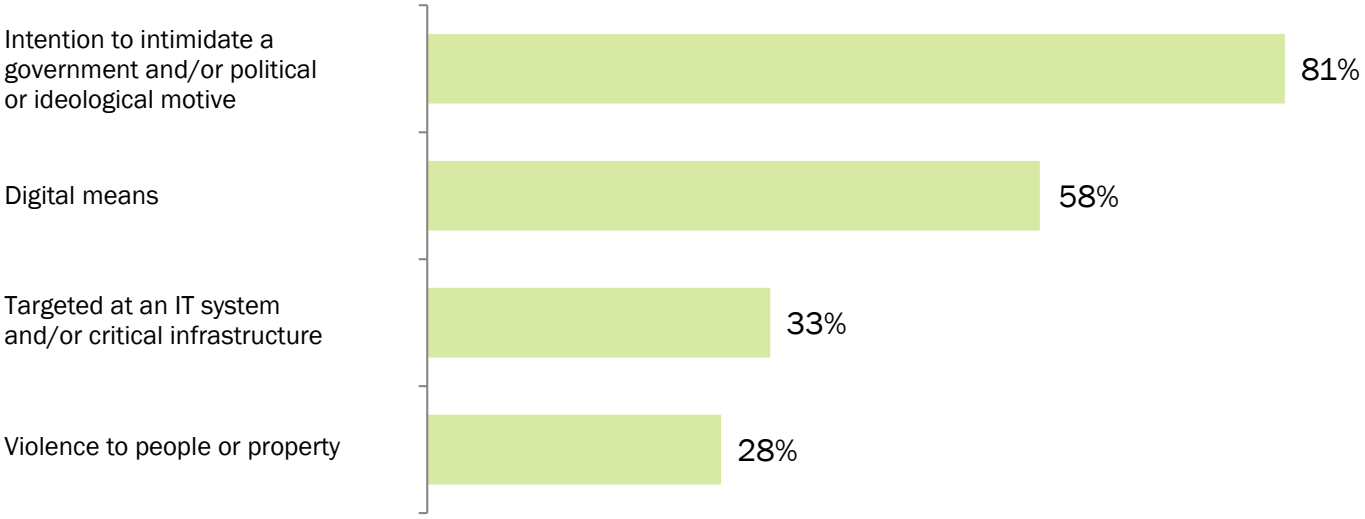
The most important factor is the means: 3 respondents.

Example: "I think the important factor is the means. Terrorists were bombing computing facilities in the 1970s and early 1980s. The term 'cyber' wasn't around back then, but I would not call them acts of cyber terrorism today" – R67.

Distinction between preparation, means and target is unclear: 3 respondents.

Which definitions of cyberterrorism, if any, do you prefer to use in your research?

43 responses were received for this question (response rate: 36%). The following chart shows the four factors most frequently cited as *necessary conditions* for an act to be classified as cyberterrorism:



The 43 responses also included:

- "Terrorism (however defined) involving a cyber element" – R82.
- "Digital warfare" – R69, R98.
- "The implementation, or threat, of hostile acts that may affect one's cyber presence" – R57.
- "I prefer to use a range of definitions that take into account both the intent and the impact of the attack" – R5.

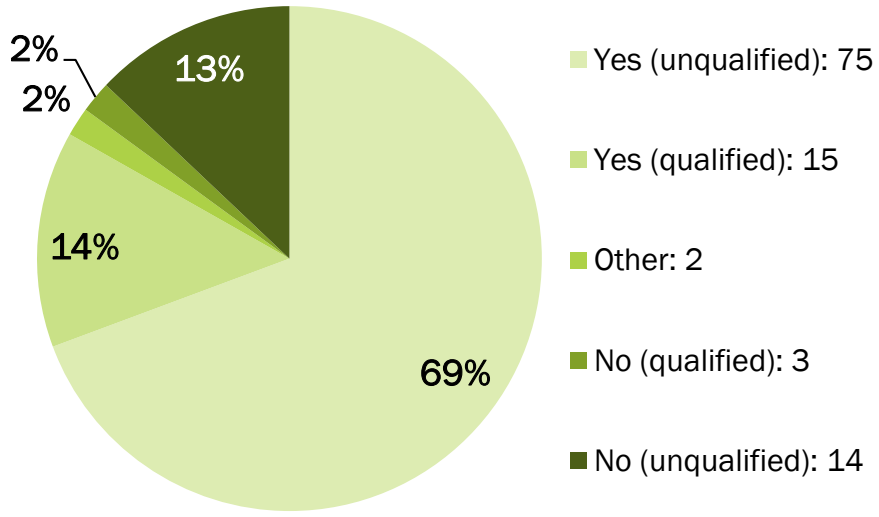
In addition to the 43 responses, a further 37 respondents stated that they either do not use the term cyberterrorism or that they purposefully choose not to define it.

> **Example**: "In all honesty, in areas like this that are evolving and challenge conventional understandings on so many levels, I don't find definitions particularly useful. I know why people try to develop them but I think that defining something like this can limit our understanding as much as it enhances it. Naturally, in one's own work a definition builds fences and creates an understanding between the author and reader about the terms of reference. But in a broader sense, I think that some of the questions you are raising here could help us better understand changing ideas about terrorism more generally (which is a socially constructed term and definition, after all). For example an answer to the question of whether states can engage in cyberterrorism could have implications for how we regard terrorism and state behaviour in a conventional sense." – R105.

One other respondent stated that they had yet to find a satisfactory definition.

In your view, can states engage in cyberterrorism?

109 individuals answered this question (response rate: 92%).



Responses were grouped into the following five categories:

Yes (unqualified).

Example: "Any social actor with sufficient knowledge, means and intent can utilise any particular tactic, be it cyberterrorism or anything else, be they states or any other social entity" – R65.

No (unqualified).

Example: "I believe actions by states are best viewed in terms of warfare/ coercive foreign policy. Reserving the term for non-state actors (even if sponsored by states) affords a certain degree of analytical clarity" – R1.

Yes (qualified).

Example: "In effect, yes, even if it should be more carefully labelled as espionage/sabotage" – R99.

No (qualified).

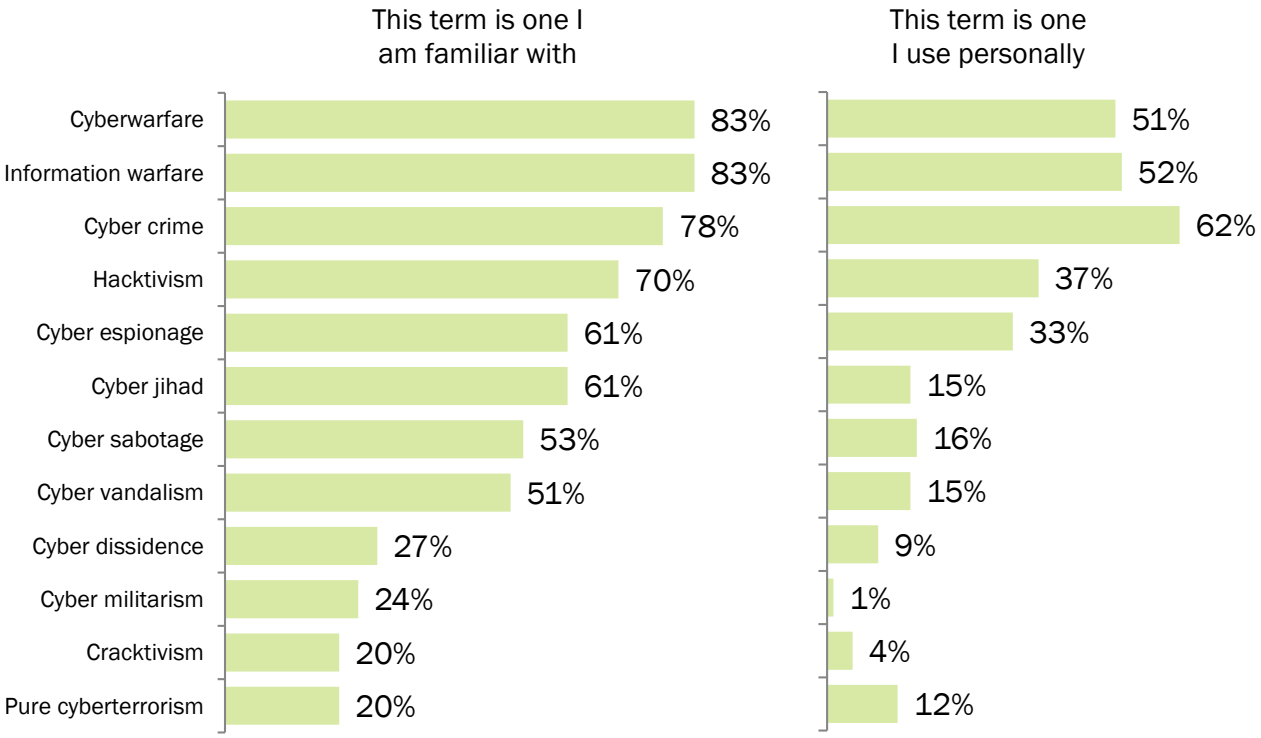
Example: "No, but they can sponsor it" – R108.

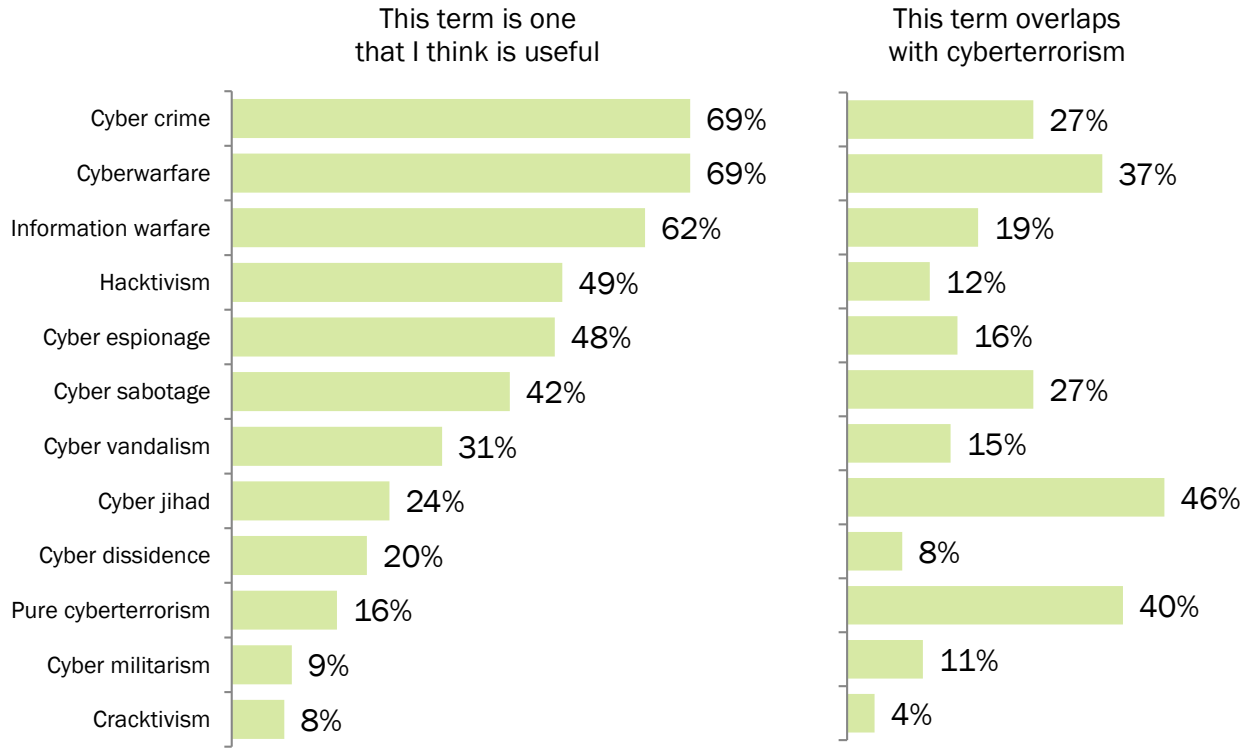
Other.

Example: "That is a great question - one [that] I think will increasingly occupy researchers and analysts. Presumably, you mean if a state engages in that behaviour, is it to be considered as terrorism or something else like state belligerence. I think a lot of people would say 'no' to your questions but of course Stuxnet prompts some reconsideration of that" – R105.

With reference to your own work, what is your experience with the following terms?

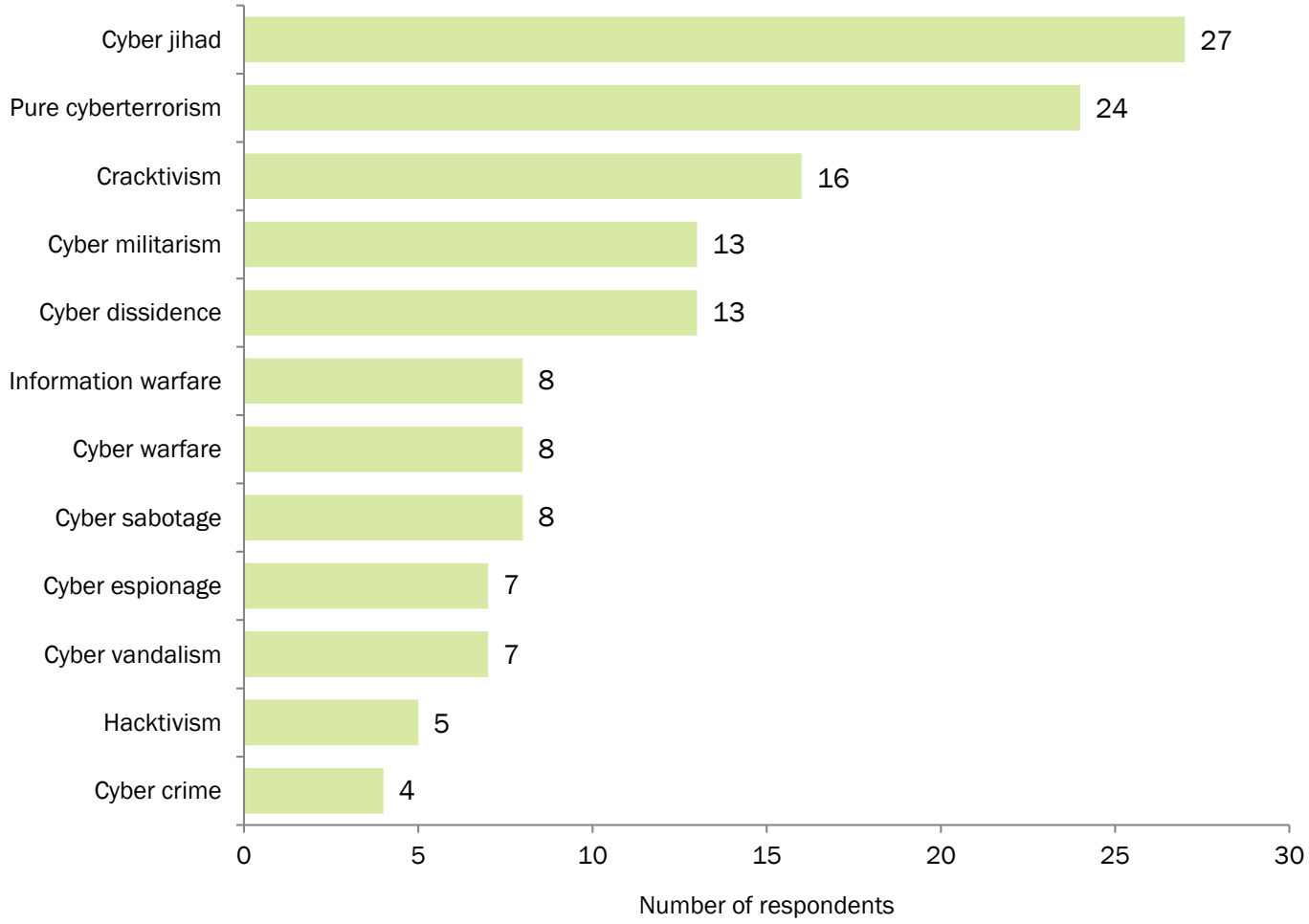
The following bar charts only include responses from the 89 respondents who completed the question in full (response rate: 75%).





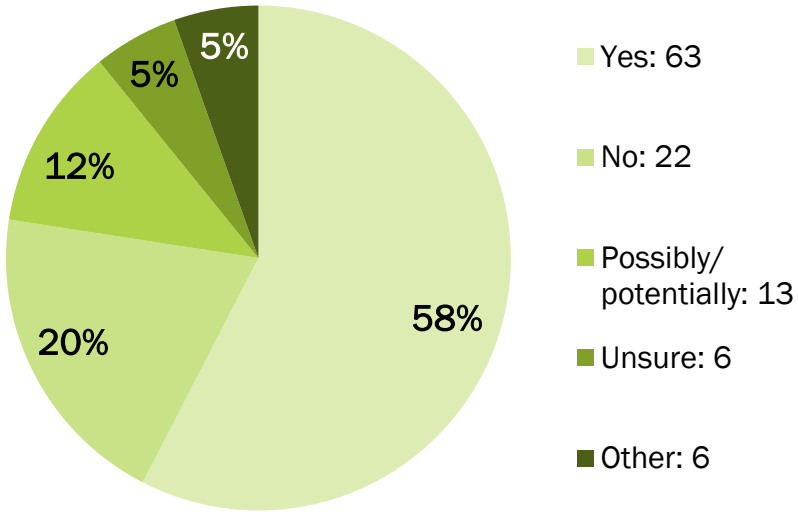
Of the terms listed on page 12, are there any which you purposefully avoid?

50 respondents stated that they purposefully avoid using one or more of the following terms (response rate: 42%).



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

110 individuals answered this question (response rate: 93%).



The following were identified as the threat's referent (some respondents listed more than one of these):

- Government/state: 23 respondents.
- Critical infrastructure/computer networks: 19 respondents.
- Civilians/individuals: 10 respondents.
- Organizations/private sector/corporations/economy: 10 respondents.
- Society: 3 respondents.
- Anyone/everyone: 3 respondents.
- Groups: 2 respondents.
- Political elections: 1 respondent.

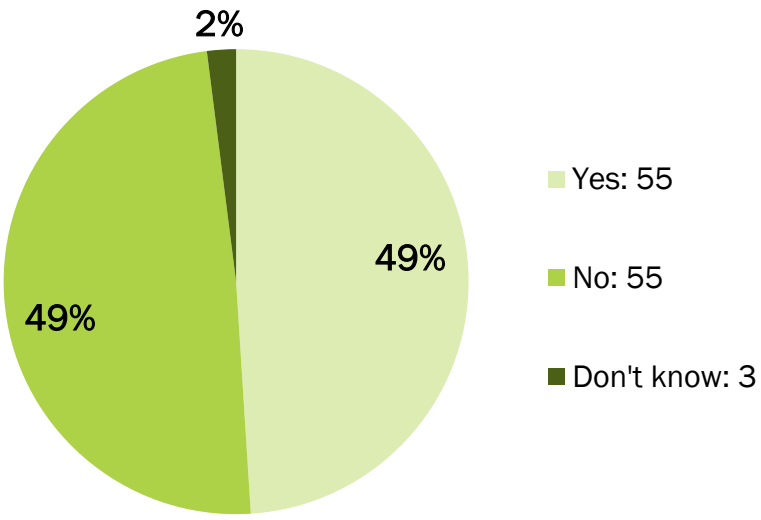
Of those that answered "no", six respondents stated that terrorists lack the capability to perpetrate cyberterrorism, and two stated terrorists lack the motivation to do so.

The "other" category contained a diverse range of comments, including:

- "It depends on who you ask" – R30.
- "It is a threat if it is constituted as such by security discourse" – R36.

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

113 respondents answered this question (response rate: 96%).



A total of 15 different incidents were identified as examples of cyberterrorism. Of these, the most frequently cited were:

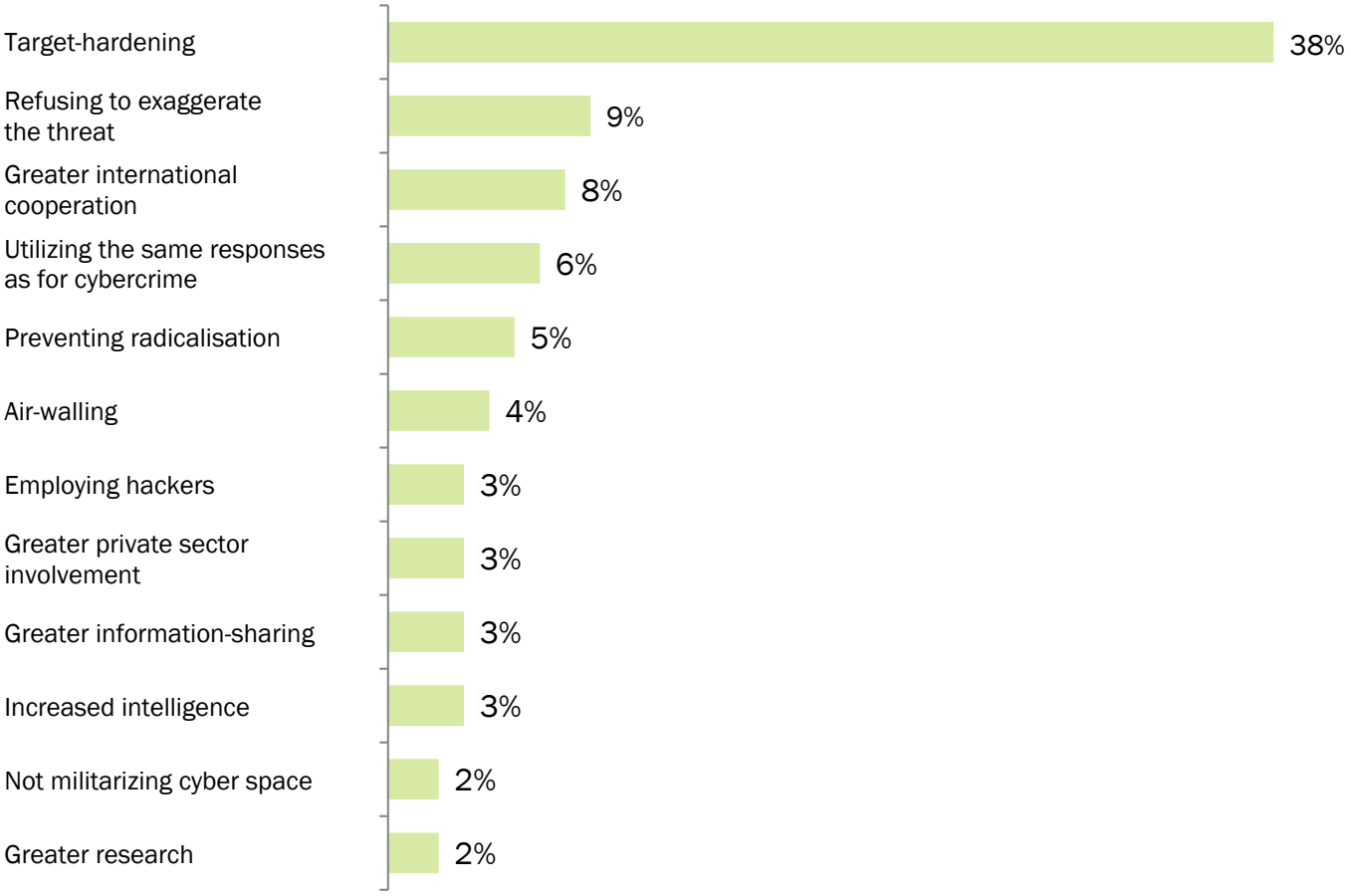
- Attacks on Estonia: 11 respondents.
- Stuxnet, Iran: 6 respondents.
- Attacks on Georgia: 3 respondents.

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

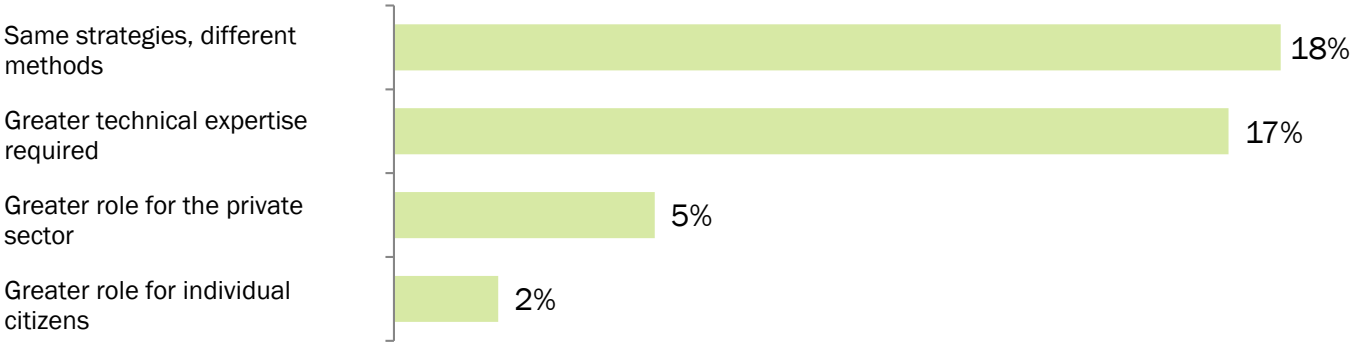
- Cyber attacks to date have not been perpetrated by non-state actors: 8 respondents.
- Cyber attacks to date have not resulted in violence against people or property: 7 respondents.
- Cyber attacks to date have been committed by perpetrators lacking the intention to create terror and/or a political motive: 6 respondents.
- There have been acts of cybercrime, but not cyberterrorism: 4 respondents.
- Terrorists do not have the capability to launch a cyber attack: 2 respondents.

In your view, what are the most effective countermeasures against cyberterrorism? Are there significant differences to more traditional forms of anti- or counter-terrorism?

93 responses were received (response rate: 79%). The following 12 measures were all identified by at least two respondents:

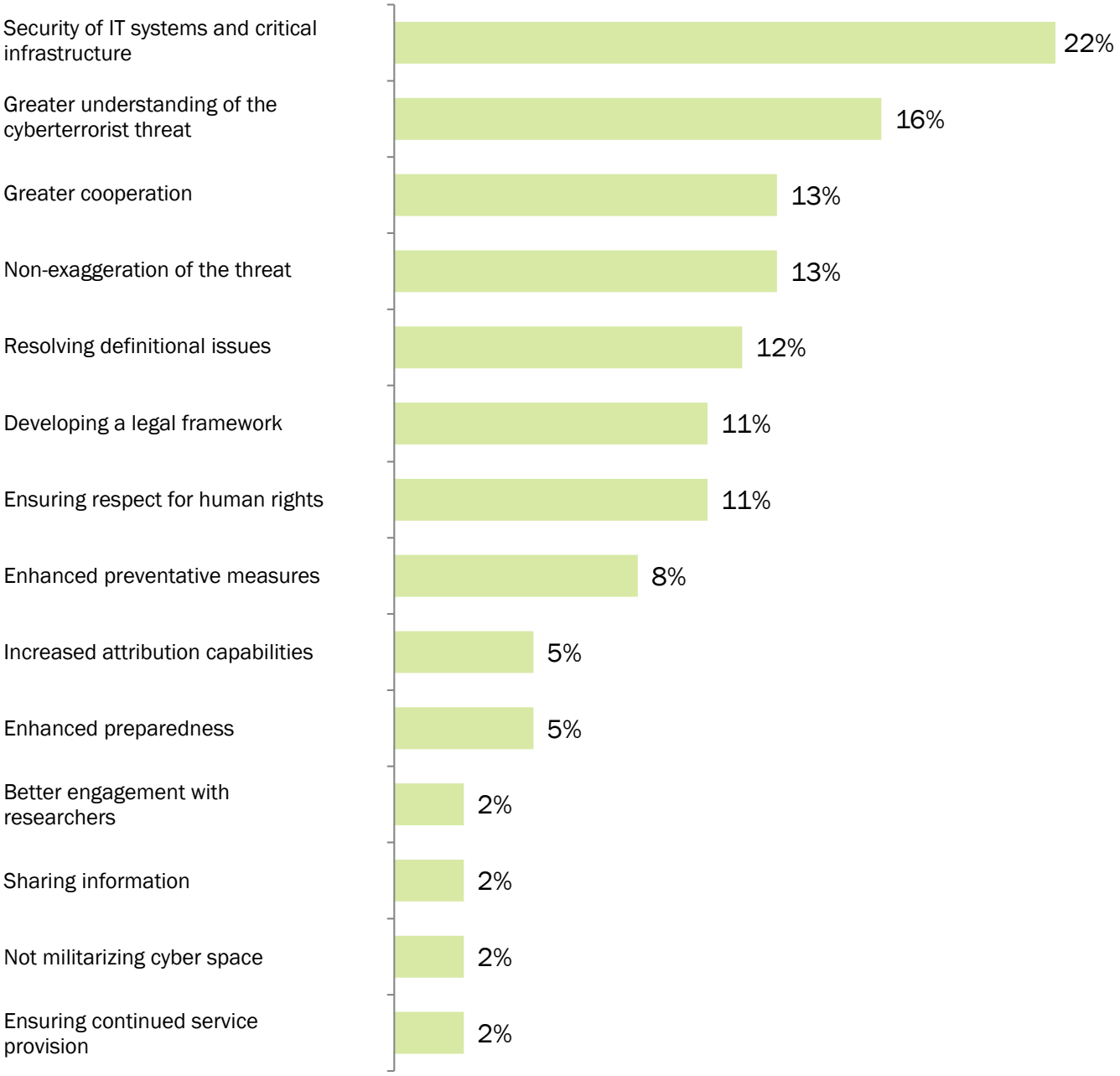


On the second half of the question, the following four responses were the most common:



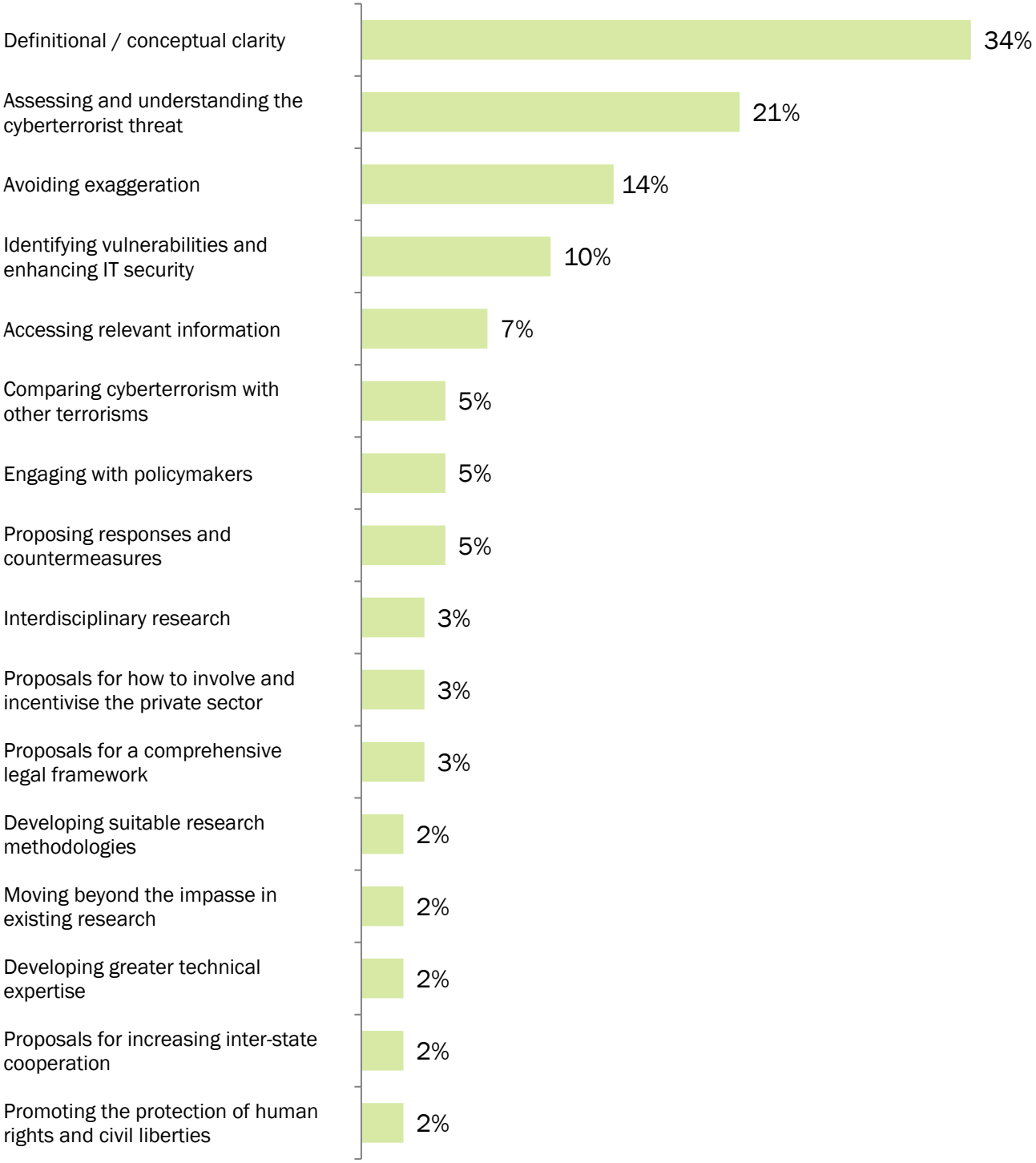
What are the most pressing issues in the field of cyberterrorism: for policymakers?

85 responses were received (response rate: 72%). Many respondents identified a number of issues.



What are the most pressing issues in the field of cyberterrorism: for researchers?

86 responses were received (response rate: 73%). Again, many respondents identified multiple issues.



In which country is your place of employment?

United States	41 (35%)	Germany	2 (2%)	India	1 (1%)
United Kingdom	32 (27%)	Ireland	2 (2%)	Kuwait	1 (1%)
Australia	7 (6%)	Italy	2 (2%)	Nigeria	1 (1%)
Canada	4 (3%)	Netherlands	2 (2%)	Portugal	1 (1%)
Israel	3 (3%)	New Zealand	2 (2%)	South Africa	1 (1%)
Switzerland	3 (3%)	Norway	2 (2%)	South Korea	1 (1%)
Czech Republic	2 (2%)	Slovenia	2 (2%)	Turkey	1 (1%)
Denmark	2 (2%)	Chile	1 (1%)	United Arab Emirates	1 (1%)

(One respondent declined to answer)

How would you classify your current employment?

Academic Staff (permanent)	75 (64%)	Academic Staff (temporary)	16 (14%)
Research Student	9 (8%)	Independent Researcher	11 (9%)
Retired	2 (2%)	None of the Above	5 (4%)

How would you classify your primary disciplinary background?

Group A:	Political Science, International Relations, et. al.	69 (50%)
Group B:	Law, Criminology, et. al.	15 (11%)
Group C:	Economics, Business, et. al.	2 (1%)
Group D:	Engineering, Computer Science, Cyber, et. al.	17 (12%)
Group E:	Psychology, Anthropology, et. al.	20 (15%)
Group F:	Literature, Arts, History, et. al.	9 (7%)
Group G:	Independent researchers, Analysts, et. al.	5 (4%)

(Some respondents listed more than one field)

Selected additional comments

A number of respondents provided additional comments. The focus of these varied considerably. Whilst some emphasised the importance of a definition of cyberterrorism, others doubted the need for a definition and even questioned the validity of the concept. A selection of illustrative comments are included below:

R1 "On the one hand definitions of terrorism will never be resolved. On the other hand working definitions of terrorism are in place which facilitate law enforcement. There will always be disagreements and difficulties in implementing CT, especially internationally. Since definitions are needed in order to implement policy and legislation, and since cyberterrorism in particular is likely to involve multiple international jurisdictions, working definitions of cyberterrorism (or at least of cyber attacks which terrorists may commit) are necessary."

R21 "Having worked in a policy-making environment as well as an academic one on this issue, it seems to me that policy-makers' definitions of such phenomena tend to flow from legislative sources and are significant only inasmuch as they affect decisions about prosecutions (i.e. who should be charged with 'terrorist' hacking vs. computer mischief) or jurisdiction (i.e. an incident is a law-enforcement problem or an intelligence-service problem). They are far more problematic and vital for researchers, who wish to understand the phenomena in question in objective, holistic terms."

R82 "The major issue is finding a definition of acceptable cyber activism--the cyber equivalent of the right to peaceful assembly, peaceful demonstrations, etc."

R36 "Security practice does not require definition of threat. It is performative - it constructs its own threats and its reasons for being. Cyberterrorism, or 'terrorism', performs an oppositional construct that doesn't require specific definition."

R15 "The concept of 'cyberterrorism' is loaded with tremendous inherent biases which vitiate it as an objective concept. It should be referred to as cybersabotage, cybercrime, cyberprotest, etc, which are much more accurate and valid concepts."

the cyberterrorism project

Contact Details

ctproject@swansea.ac.uk

www.cyberterrorism-project.org

www.facebook.com/CyberterrorismProject

@CTP_Swansea

Project Directors

Professor Thomas Chen
College of Engineering

t.m.chen@swansea.ac.uk
@TomChenTwt

Professor Thomas Chen is an expert in computer and network security. His previous research projects have explored Internet security, intrusion detection, attack modelling, malicious software and cybercrime, with support from various US agencies and companies. He is co-editor of *Broadband Mobile Multimedia: Techniques and Applications* (2008) and *Mathematical Foundations for Signal Processing, Communications, and Networking* (2011), co-author of *ATM Switching Systems* (1995), and has published papers in a number of IEEE journals including *IEEE Computer, IEEE Security and Privacy, IEEE Internet Computing,* and *IEEE Transactions on Smart Grid*.

Dr Lee Jarvis
Department of Political and Cultural Studies

l.jarvis@swansea.ac.uk
@LeeJarvisPols

Dr Lee Jarvis' research focuses on elite and non-elite understandings of terrorism, as well as the social and political impacts of counter-terrorism powers. His work is either published or forthcoming in journals including *Security Dialogue*, *Political Studies*, *International Relations*, *Critical Studies on Terrorism*, and *Citizenship Studies*. He is author of *Times of Terror: Discourse, Temporality and the War on Terror* (2009), and co-author of *Terrorism: A Critical Introduction* (2011). His most recent research project is the ESRC-funded: *Anti-Terrorism, Citizenship and Security in the UK*.

Dr Stuart Macdonald
School of Law

s.macdonald@swansea.ac.uk
@CTProject_SM

Dr Stuart Macdonald researches criminal law and criminal justice. He has written a number of articles examining frameworks for analysing and evaluating anti-terrorism policies and legislation. These have been published in leading international journals, including the *Sydney Law Review* and the *Cornell Journal of Law and Public Policy*. He has held visiting scholarships at Columbia University Law School, New York, and the Institute of Criminology at the University of Sydney. His recent project on security and liberty was funded by the British Academy.