European Insurance and Occupational Pensions Authority

PUBLIC
EIOPA-22/415
22 September 2022
FINAL

Resolution of comments

Public consultation on the Supervisory statement on management of non-affirmative cyber underwriting exposures

No	Stakeholder	Response to the public consultation	EIOPA's comments
1	AAE	Par 1.5 – The frequency and level of sophistication has increased in all sectors not just financial institutions. In particular, financial institutions have been targeted both directly and indirectly (via phishing attacks on clients, fake calls to retrieve sensitive information etc.). It should be noted that a significant number of attacks is on non-financial institutions e.g., logistical companies, airliners, car manufactures, engineering companies. Motivation of these attacks varies and go across from financial gain, "ecological" attack (disturb non-environmentally friendly companies to operate), theft of the intellectual property, etc. In the current environment large companies present the target for the cyber criminals, however with the level of sophistication and potential for higher scale, SMEs may start to become more targeted due to lower levels of security and awareness. This may become a test for the insurance market and for how various policies respond to those type of business interruption / blackmail attacks,	Agree. A footnote regarding the topic has been added to the Supervisory Statement.
2	AAE	Par. 1.6 - The environment of instability may result in a proliferation programming code for highly effective cyberattacks.	Agree. EIOPA intentionally avoided reference to technical aspects of sophistication of cyber attacks as this goes beyond the scope of the Supervisory Statement, but indeed these aspects should be kept in mind by undertakings when performing exposure assessment.

No	Stakeholder	Response to the public consultation	EIOPA's comments
3	AAE	Par. 17.7 - It is true that the (re)insurance sector may play a facilitating role for digital transformation to reduce the protection gap. However, the vast and unforeseeable accumulation risk that stems from the fact that many retail clients make use of very similar infrastructure. This is a decisive limitation of the sector's ability to help to close the protection gap. A Member state or EU guaranteed pool solution for high excess event losses will be necessary to enable the sector to play its foreseen role. Another limiting factor for the risk management function of the sector arises from the fact that the cyber-attack space is moving extremely fast.	Noted. EIOPA overall shares the concerns on the protection gap and the need for some sort of shared resilience solution moving forward, however the considerations regarding the use of risk pools go beyond the scope of the Supervisory Statement. On the pace of evolution associated with cyber risks, EIOPA fully agrees and believes that one way to address this issue is the implementation of continuous risk monitoring schemes (as described in the "Supervisory Expectations" section of the Supervisory Statement.
4	AAE	Par. 1.9 - Cyber insurance is still a relatively new product and as a society we are still learning the way how cyber attack can impact one's business or life. Even the current specific cyber insurance policies cover some element of cyber risk, but might include other – e.g., war, state funded cyber attackscyber-attacks. A move to cyber covers that are both, affirmative and well defined in terms of in- and exclusion of war-like or state agency driven cyberattacks seems reasonable.	Noted. EIOPA agrees with the description provided and believes the messages conveyed by the Supervisory Statement go in this direction.
5	AAE	Par. 1.10 - Insurance market is continuously evolving despite the current lack of appetite for the cyber exposure or cyber war exposure. It might change in the future; however, in the interim some elements of state funded cyber war pools might encourage insurers to offer such products, given they will have ability to mitigate the overall risk, whilst learning about the risk itself, which will ultimately promote higher appetite towards such risk, if the risk/reward is in reasonable balance. Precise and robust contract language seems necessary to avoid lengthy court deliberation. It seems obvious that the sector cannot cover large scale cyber-attacks, regardless if it could be classified as an act of war of not. Modern cyber-attacks are difficult to attribute to a state or a state agency. The necessary evidence is unlikely to be producible in court, due to military secrecy. War exclusion type of contract clauses are therefore less likely to be effective.	Agree. EIOPA believes that, together with the evolution of risks and threat landscape, further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium in supply and demand.
6	AAE	Par. 1.11 - This might be a huge task. Significant amount of products have not been developed with cyber risks in mind, however clients likely have a different understanding after such claim has occurred. The situation is somewhat similar to pandemic/epidemic covers. Before Covid-19 pandemic not many insurers/reinsurers were even thinking about	Agree. The links with the COVID19 pandemic have also been identified throughout the Supervisory Statement.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		the possibility of clients claiming the Covid-19 business interruptions claims on their property insurance as that product was not designed for it. Others were convinced that the condition of a property damage to trigger the BU loss was ruling out any cover in most jurisdictions. Similarly, many policies with silent cyber exposure can be subject of different interpretation and claims litigation.	
7	AAE	Par. 1.12 - We feel that EIOPA's broader mission to promote sound technological progress for the benefit of the European Union economy and its citizens must include an analysis of the main obstacles for the sector to help to close the protection gap. We must address the vast and unforeseeable accumulation potential that stems from the fact that many clients make use of very similar infrastructure. It is hard to see, how this could be addressed without a statutory limitation of the total per event or series of events loss for the sector and some societal cover for the excess.	Agree. Addressing the issue of the protection gap is included in EIOPA's objectives and will further work on it, however it goes beyond the scope of the Supervisory Statement. EIOPA suggests joint reading of both the Supervisory Statement on Exclusions and Management of non-affirmative cyber exposures.
8	AAE	Par. 1.13 - There is no easy way to identify exposure toward cyber in silent cyber covers. It would be beneficial if EIOPA would provide market with some guidance, so there is some level of consistency across the European/non-European market (e.g., many European domiciled clients insure/reinsure non-European business).	EIOPA believes that the principles outlined in the Cyber Underwriting Strategy and in the Supervisory Statement, such as the need for undertakings to define a plan to identify and manage non-affirmative cyber underwriting risk, including tailored considerations regarding the specificities of the multiple Lines of Business and products impacted sets out the overall principles along which the industry should move to build a sound market for cyber underwriting. Regarding the level of consistency across EU-non-EU markets, it should be noted that territorial specificities, including consumers culture (e.g. more privacy protection-oriented rather than business interruption-oriented) play an important role. EIOPA will continue playing its role for ensuring an equal level playing field for the EU (re)insurance market.

No	Stakeholder	Response to the public consultation	EIOPA's comments
9	AAE	Par. 1.14 - Especially regarding c), it must be noted that there is a lack of cyber exposure reinsurance capacity on the market, so insurers with large "non-affirmative" cyber exposure might be struggling to find appropriate reinsurance as the level of exposure will be highly uncertain. Moreover, it is believed that many insurers /reinsurers will start explicitly excluding the cyber exposure from their policies and offer separate "carefully worded" cyber cover. However, the principal limitation of insurance and reinsurance cover due to the vast and unforeseeable accumulation potential of cyber risk will not be addressed by these measures alone, see our comment to 1.12.	Agree. One sentence on the monitoring of the reinsurance offering has been added to paragraph 1.27. Good risk management is also about adapting underwriting strategies to reinsurance capacity.
10	AAE	Par. 1.15 - We feel it is important to stress that this should apply regardless of whether cyber explicitly covers are affirmative or not.	Agree. This is indeed the message conveyed by the paragraph.
11	AAE	Par. 1.16 - We feel it is important to stress that this should apply regardless of whether cyber explicitly covers are affirmative or not.	Agree. This is indeed the message conveyed by the paragraph.
12	AAE	Par. 1.17 - This is very difficult to do in practice and it may be even harder to do with consistently. Insurers will very unlikely see a scenario where cyber claim can hit e.g., car insurance as it hasn't been priced for it and accounted for. Therefore, sharing best practices will be key. Moreover, where an insurer considers that there is a potential exposure toward non-affirmative cyber exposure, this must not set any prejudice to the question if a client might be able to claim on such cyber silent cover. Otherwise the risk management activity itself may become risky.	Partially agree. EIOPA believes that, even facing difficulties, undertakings should apply an evolving mind-set regarding raising staff awareness, even across functions. An additional sentence on the importance of sharing of good practices has been added to the paragraph.
13	AAE	Par. 1.18 - There is currently very limited amount of cyber related accumulation systems, so levels of overall cyber risk exposure will be highly spurious, at least in the beginning. Sharing best practices will therefore be key.	Noted. On the sharing of good practices, please refer to the sentence added to the previous paragraphs.
14	AAE	Par. 1.19 - We feel that a by-product of this process might be significant need for explicit cyber reinsurance covers, but capacity is unlikely not meet the demand. This in turn might lead to exclusions and thus to a widening of the protection gap for customers and the economy. NCA or EIOPA should be ready for increased demand and help the sector to meet the demand. They must help to address the vast and unforeseeable accumulation potential that stems from the fact that many clients make us of very similar infrastructure. It is hard to see, how this could be addressed without a statutory limitation of the total per event or series of events loss for the sector and some societal cover for the excess. As many policyholders might not be currently aware of the existing cyber protection gap, but there will be no suitable product on the market which would satisfy their needs.	EIOPA believes that further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand, thus ultimately generating request for increased capacity. Also, addressing the issue of the protection gap is included in EIOPA's

No	Stakeholder	Response to the public consultation	EIOPA's comments
			objectives and will further work on it, however it goes beyond the scope of the Supervisory Statement. A joint reading of the Supervisory Statement on management of non-affirmative cyber exposures and the Supervisory Statement on exclusions should give an overview on the topic of exclusions.
15	AAE	Par. 1.20 - In the current environment post pandemic, soaring energy costs, inflation and interest rates often hitting 40 years high. It might not be possible for the policyholders to adopt all measures set out by insurers and ultimately would become uninsurable. EIOPA and NCA should have some plan how to bridge the gap in the interim. The vast and unforeseeable accumulation potential that stems from the fact that many retail clients make us of very similar infrastructure further engraves the situation. It is hard to see, how this could be addressed without a statutory limitation of the total per event or series of events loss for the sector and some societal cover for the excess.	EIOPA believes that such considerations should also be taken into account when performing the quantitative and qualitative analyses regarding cyber exposures.
16	AAE	Par. 1.25 - It might be beneficial, if EIOPA would lead the efforts to unify the terminology and wording regarding cyber exposure across the European market. Overall, the market and consumers would benefit with standardization of terms and conditions, which would allow policyholder to compare individual products and ultimately shift the policyholders' attention from "cheapest" product to the "quality and needs meeting" product.	Noted. Already in the Cyber Underwriting strategy, EIOPA identified for itself the role of facilitator when it comes to the development of a sound cyber underwriting market.
17	AAE	Par. 1.26 - Cyber exposure is relatively new, and any accumulation system is subject to high uncertainty. EIOPA such mitigate these uncertainties by sharing best practises. Otherwise, as such the resulting prudency loading might be punitively high, which would ultimately prevent insurers to deploy more capacity towards cyber products.	Agree. A clarification sentence has been added on the risk of overpricing of products.
18	AAE	Par. 1.27 - Currently the cyber reinsurance capacity is very limited and if placed the rates are very high, mainly due to overall uncertainty of the clients' "silent" exposure and generally understanding the underlying exposure and its cyber exposure. Moreover, the exposure from different ceding companies do not diversify on the insurer's balance sheet. To facilitate that more capacity is to be deployed, NCA/EIOPA might need to consider some element of state-funded pools (e.g., Flood Re, Terrorism covers TRIA etc.) to help market understand the exposure, update their T&Cs, educate clients and develop suitable products. Some elements of state funded protection might help insurers to do all above in a controlled/risk	EIOPA believes that further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand, thus ultimately

No	Stakeholder	Response to the public consultation	EIOPA's comments
		mitigated environment, whilst actively working with clients to close the cyber protection gap.	generating request for increased capacity. EIOPA overall shares the concerns on the protection gap and the need for some sort of shared resilience solution moving forward.
19	BIPAR	Par. 1.6 - An example of "environment of instability" is the recent development of territorial exclusions by insurers.	Agree. A sentence of clarification regarding this topic has been added to the paragraph.
20	BIPAR	Par. 1.8 - Strong awareness of "silent cyber", flexibility of carriers and good understanding of cyber risk and its consequences is necessary to ensure no gap.	Agree. EIOPA believes the messages conveyed by the Supervisory Statement should help to this end.
21	BIPAR	Par. 1.13 - Each product and line of business is different. Cyber should be addressed very carefully and in function of different lines of business. (Professional indemnity, medical malpractice, D&O, Marine, Aviation, Property, Terrorism … The list is long, but the considerations possibly need to be specific.	Noted. Additional specification regarding this aspect has been added to the paragraph.
22	BIPAR	Par. 1.24 - Documenting the scenarios when developing the product is essential so there is no misunderstanding in the channel of communication: developer – underwriter – intermediary – client. With that "information and advertising material", everyone would need to be on the same page.	Noted. Additional specification regarding this aspect has been added to the paragraph.
23	BIPAR	Par. 1.28 - Are there many disputes around terms and conditions in cyber claims in Europe? Are the known triggers not clear enough? Losses that are too big to be sustained for the insurance industry are under increasing focus of insurers (they may not be covered anyway because insurers may not be in a position to be able to pay the claims) Removing all "systemic" risk to cyber insurance may lead to the end of this line of business which is more and more perceived as an important tool to fight against cyber threat, alongside cyber security, cyber awareness.	The potential systemic nature of cyber risks is embedded in their nature and therefore cannot be isolated. EIOPA calls for acknowledgement of the systemic potential rather than attempt to isolate this component.
24	BIPAR	Question 2 - Identification and measurement of risks exposure with the purpose of implementing sound cyber underwriting practices, with particular regard to the non-affirmative cyber risk.	Noted.
25	BIPAR	General Comments - For insurance intermediaries clear pre-contractual and contractual information is key.	Already in the Cyber Underwriting strategy, EIOPA identified for itself the role of facilitator when it comes to the

No	Stakeholder	Response to the public consultation	EIOPA's comments
		It would be useful if EIOPA could add a glossary /definition of some key terms used in the paper, for example the definition of cyber risk. To the best of our knowledge EIOPA "defines" cyber risk as follows: Cyber risks are "the combination of the probability of cyber incidents occurring and their impact". According to the Cyber Lexicon of the Financial Stability Board (FSB). The problem is that this is a circular definition and further EIOPA only refers to FSB Cyber lexicon. Can we derive from that, that the EIOPA paper when using the word cyber risks refers to the FSB definition or does EIOPA has its own definition? According to IAIS, the definition of cyber risks is "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information − be it related to individuals, groups, or governments." We were wondering if it would be useful to include a paragraph on systemic cyber cover? This may be dealt with in the systemic paper but cyber is different from, for example, natural Catastrophes. Cyber may have consequences on many risks (supply chain related insurances, transport, etc).	development of a sound cyber underwriting market but does not see its role as setting glossaries and definitions rather than facilitating the sharing of commonly used taxonomies. As mentioned in the comment, the FSB Lexicon might be a good reference for industry, even though more precise definitions would need to be tackled by the undertaking also taking into account the products' specificities.
26	FERMA	Par. 1.5 - FERMA agrees that cyber exposures are a worthy area of focus for EIOPA. According to risk managers we have surveyed over the past 6-8 years at least, the cyber threat is the most pressing concern of all risks, at least in the near-term. In 2022, in our most recent addition of the European Risk Manager Report, it is clear that cyber threats dominate all over concerns. https://www.ferma.eu/risk-managers-in-a-time-of-transitionresults-of-the-ferma-european-risk-manager-survey-2022/ Furthermore, we also should state that exclusions in insurance contracts, as well as ambiguities in wording and clauses are both problems for clients of insurers. See, for instance, there is a well-document problem from the client perspective in the new LMA set of exclusions as documented by Marsh here: https://www.marsh.com/us/services/cyber-risk/insights/new-cyber-war-exclusion-language-raises-concerns.html	Noted. EIOPA welcomes the development of such initiatives across the EU market and encourages the sharing of good practices among professionals.
27	FERMA	Par. 1.7 - FERMA fully agrees with the point made here. We emphasise that the protection gap is a real concern among corporate insurance buyers. According to the recent findings of	Agree. EIOPA welcomes the development of such market analysis initiatives across

No	Stakeholder	Response to the public consultation	EIOPA's comments
		Project LUCY - which is an initiative launched by FERMA member AMRAE, the French risk management association - in 2021, there was less coverage available for cyber at a higher premium. More specifically, coverage rates fell by 4.4% for large enterprises whereas average premium volumes rose by 44.4%. FERMA is also anticipating to receive figures from the Belgian and Italian markets and will keep EIOPA informed of how this exercise progresses, and when the figures are available.	the EU market and encourages the sharing of good practices among professionals.
28	FERMA	Par. 1.8 - FERMA agrees in general that exclusions and ambiguous terms in insurance contracts are problems. It might also be the case that an exclusion in one line of cover would then lead to a complete gap opening up in coverage for that risk. That is a serious problem for corporate insurance buyers in their risk and insurance management. However, it is our assessment that non-affirmative cyber coverage is not the main problem in the market - , especially not for insurance buyers. The problem is actually the gap between the demand for and supply of cyber insurance coverage. Companies would like to be able to have more coverage in cyber, but the supply does not match the needs of the market.	EIOPA overall shares the concerns on the protection gap and the need for some sort of shared resilience solution moving forward. A joint reading of the Supervisory Statement on management of non-affirmative cyber exposures and the Supervisory Statement on exclusions should give an overview on the topic of exclusions.
29	FERMA	Par. 1.11 - FERMA voices its concern here that this focus may lead to some un-intentend and adverse consequences for buyers. To elaborate, our members are increasingly concerned that making "affirmative" some cover in one line of coverage will lead to that specific risk being not covered at all. Another concern is that the scrutiny placed by supervisors on insurers will ultimately lead to more exclusions in coverage. This is a serious concern on part of risk and insurance managers.	EIOPA believes that further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand, thus ultimately generating request for increased capacity. However, the statement does not aim at encouraging the over-use of transformation of non-affirmative coverages into exclusions or unclear affirmative coverages, but rather on good risk management practices to help the development of a sound market for cyber underwriting. A clarification sentence has been added to the introduction to the Supervisory Statement.

No	Stakeholder	Response to the public consultation	EIOPA's comments
30	FERMA	Par. 1.13 - FERMA voices its concern here that this focus may lead to some un-intentend and adverse consequences for buyers. To elaborate, our members are increasingly concerned that making "affirmative" some cover in one line of coverage will lead to that specific risk being not covered at all. Another concern is that the scrutiny placed by supervisors on insurers will ultimately lead to more exclusions in coverage. This is a serious concern on part of risk and insurance managers.	The statement does not aim at encouraging the over-use of transformation of non-affirmative coverages into exclusions or unclear affirmative coverages, but rather on good risk management practices to help the development of a sound market for cyber underwriting. A clarification sentence has been added to the introduction to the Supervisory Statement.
31	FERMA	Par. 1.15 - FERMA voices its concern here that this focus may lead to some un-intentend and adverse consequences for buyers. To elaborate, our members are increasingly concerned that making "affirmative" some cover in one line of coverage will lead to that specific risk being not covered at all. Another concern is that the scrutiny placed by supervisors on insurers will ultimately lead to more exclusions in coverage. This is a serious concern on part of risk and insurance managers.	The statement does not aim at encouraging the over-use of transformation of non-affirmative coverages into exclusions or unclear affirmative coverages, but rather on good risk management practices to help the development of a sound market for cyber underwriting. A clarification sentence has been added to the introduction to the Supervisory Statement.
32	FERMA	Par. 1.23 - While FERMA agrees entirely with the fact problems exist in terms of affirmative vs non affirmative and exclusions in coverage more broadly, it is our assessment that tackling non-affirmative cover may not be the surest way to achieve it, since we fear as insurance buyers that the private insurance market would treat the supervisory statement as a means to exclude more and cover less. It is our firm belief that further investigated the needs of the client/insured (ie what coverage is needed) and the reasons for the lack of supply will lead to more beneficial outcomes for the cyber insurance market.	Noted. EIOPA believes that further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand, thus ultimately generating request for increased capacity.
33	FERMA	Question 2 - FERMA supports the initiative taken by EIOPA around cyber insurance coverage. Risk managers assess cyber threats to be the top-risk for organisations over a number of years. There are clearly problems with insurance coverage.	Noted. EIOPA overall shares the concerns on the protection gap and the need for some sort of shared resilience solution moving forward. EIOPA believes that further clarity in exposures and policy wording might result in clearer

No	Stakeholder	Response to the public consultation	EIOPA's comments
		Nevertheless, FERMA' main concern is not related to non-affirmative (or silent) coverage. The problem is actually the gap between the demand for and supply of cyber insurance coverage. Companies would like to be able to have more coverage in cyber, but the supply does not match the needs of the market. AMRAE results. EIOPA's focus on making insurers move their coverage to more affirmative risks may have a harmful effect on insurance buyers. It may lead to even more exclusions, and even less coverage overall with more gaps opening up. This trend is even more worrying for SMEs. For larger companies there is still a market for insurance. But SMEs not. According to figures from France, there is a 325% claim ratio for SMEs in France in 2021. This will likely lead to more and more SMEs to either withdraw massively from the cyber insurance market or the coverage will just be completely unaffordable. On top of this, as shown by eg premium volume collected in France, it is the large companies' premium that makes the market. At same time SMEs are without coverage, increasingly, large companies are withdrawing. This makes the issue even more pressing for SMEs. (see Project LUCY findings: https://www.amrae.fr/recherche?search_api_fulltext=lucy)	information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand, thus ultimately generating request for increased capacity.
34	FERMA	Question 4 - It is FERMA's assessment that this may not achieve the desired effects It would seem the market has more exclusions and less coverage than before and it is possible that this would deteriorate yet further for insurance buyers.	The statement does not aim at encouraging the over-use of transformation of non-affirmative coverages into exclusions or unclear affirmative coverages, but rather on good risk management practices to help the development of a sound market for cyber underwriting. A clarification sentence has been added to the introduction to the Supervisory Statement.
35	FERMA	General Comments – 1) We welcome EIOPA looking further into the protection gap regarding cyber insurance. 2) But, we assess that the focus is possibly misplaced. It is our view that in fact the major problem confronting insurance buyers is the increasing gap between demand for (i.e. protection needed) and the (lack of adequate) supply of cyber insurance.	Noted. EIOPA welcomes the support to the actions undertaken so far (e.g. issuance of the Cyber Underwriting Strategy and of this Supervisory Statement and encourages Stakeholder to get in touch to discuss further on the topic.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		3) The problems we have described above are all the more concerning for SMEs. Based on our knowledge, it is largely large corporate insurance buyers that purchase cyber insurance coverage (making the market). The few SMEs that do purchase cyber insurance coverage are increasingly challenged because it's a) expensive and b) retreating. If big corporates start walking away from purchasing cover (as is case in France) this may make it even more difficult for SMEs and that's a systemic concern. 4) On top of this, we are actually worried as a community of insurance buyers that there may be further exclusions in cyber insurance coverage added by cyber insurance carriers as a result of this supervisory statement. 5) It is FERMA's view that EIOPA should continue to look into the cyber insurance protection gap but from a perspective that is more attractive to the insured. In this context, we would be very supportive of EIOPA looking further into better understanding the demand needs of clients and the supply determinants of insurers.	
36	French Insurance Federation	Par. 1.5 - The frequency and sophistication of cyber incidents across all sectors has increased substantially, however this is due in large part to the rise of the Ransomware as a Service (RaaS) business model. While Covid-19 accelerated society's reliance on digital infrastructure, with opportune cyber criminals conducting pandemic-related phishing campaigns, it also had a positive effect on the level of cyber awareness across society as a whole.	Agree. A footnote regarding this has been added to the text.
37	French Insurance Federation	Par. 1.6 - Russia's invasion of Ukraine has most certainly contributed to the environment of instability around the world. However, this environment of instability in cyberspace is not new, nor related specifically to the war, as state-linked cyber criminals from Russia and other countries have been engaged in hostile activity in cyberspace for many years. Furthermore, while industries remain on high alert, the expected steep increase in malicious cyber activity linked to the war has so far not materialised.	Agree. A sentence of clarification regarding this topic has been added to the paragraph.
38	French Insurance Federation	Par. 1.7 - The (re)insurance sector has a role to play in increasing awareness of cyber risk and promoting sound risk management measures among prospective insureds. The sector is part of many initiatives to raise awareness of cyber risks, which is fundamental to increasing resilience. For entities seeking to increase their resilience, cyber insurance can be part of the solution. However, risk management begins at the level of the entity, and insurers usually expect entities to take control over their exposures and implement a checklist of minimum cybersecurity measures as a precondition for purchasing cyber insurance. Cyber insurance should be seen as only one of a range of tools available for retail and corporate clients to	Agree. This messages are also conveyed thought the Supervisory Statement. A footnote has been added to further clarify the topic.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		use in increasing their cyber resilience, complementing the measures implemented at the level of the entity. The role of the insurers is more necessary for the retail clients as they require most support in terms of prevention and cover.	
39	French Insurance Federation	Par. 1.8 - Cyber risk exposures are indeed under increasing scrutiny due to potential ambiguous terms and conditions in some policies. However, the sentence beginning "In fact…" should be amended in light of the following points: • "Affirmative cyber insurance policies" is a redundant term given that, by definition, a cyber policy affirmatively covers cyber risk. The word "affirmative" could be replaced by the word "dedicated". • The sentence "affirmative cyber insurance policies or cyber endorsements" implies that a cyber endorsement is not an affirmative cyber policy, which is incorrect.	No change. EIOPA believes that the definitions provided better fit for the purpose and follow commonly-used terminology.
40	French Insurance Federation	Par. 1.9 - We agree on the definition of non-affirmative cyber covers. Non-affirmative cyber exposure leading to uncertainty in coverage can indeed lead to legal uncertainty, that is why, as explained above, French insurance sector is taking action to address non affirmative cyber risk in casualty and property policies in order to comply with prudential requirements as well as in line with national supervisory recommendations.	Noted.
41	French Insurance Federation	Par. 1.10 - The treatment of war risk in cyber insurance policies is under increased scrutiny, particularly in light of current events. Discussions are ongoing in some markets to update traditional legal war exclusions to accommodate war of a cyber nature. Work has also been carried out by the Geneva Association in the area of attribution, where a new term 'Hostile Cyber Activity' has been coined to sit between cyber terrorism and cyber war, with the intention that, going forward, such a term may assist in distinguishing between what is insurable and what is not. We are in the opinion that Member States should think about updating traditional legal war definition in order to include its new aspects such as the cyber war. Indeed, a conventional exclusion could lead to legal uncertainty and source of litigation. In France the article 121-8 of the French code of insurance excludes war risk (traditional war). The Haut Comité Juridique De la Place financière de Paris (HCJP), wrote in its report about the need to start adapting this article to cyber wars as well (HCJP « Report on the insurability of cyber risks », 28 january 2022, [https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf].).	Agree. A sentence of clarification regarding this topic has been added to the paragraph.

No	Stakeholder	Response to the public consultation	EIOPA's comments
42	French Insurance Federation	Par. 1.11 - As expressed above, insurance undertakings are already doing a deep work to identify non-affirmative cyber exposure and coverage. The ACPR is strongly invested in this issue and has produced a press release the 12th of November 2019, which draws the attention of insurers on the subject (ACPR, Press Release « The distribution of guarantees against cyber risks by insurers », [https://acpr.banque-france.fr/sites/default/files/medias/documents/20191112_cp_bilan_cyber_assurance.pdf], 2019.)	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
43	French Insurance Federation	Par. 1.13 - As expressed above, considering the fact that our NSA dedicate sufficient attention to the supervision of cyber underwriting risk, we are in the opinion that there is not a specific need on this issue; in case of an EIOPA initiative, we would be in favour of the development of high-level principle provisions which are less prescriptive and more flexible.	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
44	French Insurance Federation	Par. 1.16 - We fully agree with this statement.	Noted.
45	French Insurance Federation	Par. 1.17 - We fully agree with this statement.	Noted.
46	French Insurance Federation	Par. 1.18 - We fully agree with this statement.	Noted.
47	French Insurance Federation	Par. 1.19 - As expressed above, insurance undertakings are already doing a deep work to identify non-affirmative cyber exposure and coverage. The ACPR is strongly invested in this issue and has produced a press release the 12th of November 2019, which draws the attention of insurers on the subject (ACPR, Press Release « The distribution of guarantees against cyber risks by insurers », [https://acpr.banque-france.fr/sites/default/files/medias/documents/20191112_cp_bilan_cyber_assurance.pdf], 2019).	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
48	French Insurance Federation	Par. 1.20 - As expressed above, insurance undertakings are already doing a deep work to identify non-affirmative cyber exposure and coverage. The ACPR is strongly invested in this issue and has produced a press release the 12th of November 2019, which draws the attention of insurers on the subject (ACPR, Press Release « The distribution of guarantees against cyber risks by insurers », [https://acpr.banque-france.fr/sites/default/files/medias/documents/20191112_cp_bilan_cyber_assurance.pdf], 2019)	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
49	French Insurance Federation	Par. 1.21 - The multidisciplinary approach of the risk control is a key element. The economical digitalization has great impact in all branches (property, liability, fraud...). It is essential for this risk to be studied from a transversal approach including risk prevention.	Noted. EIOPA agrees on the transversal nature of risks and already in the Cyber Underwriting strategy, EIOPA identified for itself the role of facilitator when it

No	Stakeholder	Response to the public consultation	EIOPA's comments
		It is also important for insurers, reinsurers and policyholders to share common cyber terminology developed by public authorities. Indeed, as EIOPA highlights, the lack of data to approach a risk is a major handicap. French public authorities are reflecting on the possibility of a national observatory of cyber risks.	comes to the development of a sound cyber underwriting market.
50	French Insurance Federation	Par. 1.22 - Regarding war, Following the HCJP report, national authorities should think about updating traditional legal war definition in order to include its new aspects such as the cyber war. Regarding terrorism, there is in France an obligation to cover material damages following a terrorist attack which can also be a cyber event. (Article L126-2 of the French insurance Code)	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
51	French Insurance Federation	Par. 1.23 - We fully agree on this assertion; the work undertaken by our members regarding non affirmative cyber coverages makes clear the willingness to improve terms and conditions in order to make them clear and simple.	Noted.
52	French Insurance Federation	Par. 1.24 - If any information is to be given it may only concern the main risks and the exclusions related to standalone cyber insurance products. By the way, we don't understand the reference to "consumers" as cyber coverages are mainly underwritten by professionals.	The wording "consumers" refers to any type of policyholder, being it a B2B type of customer relationship or with natural persons.
53	French Insurance Federation	Par. 1.26 - France assureurs agrees with the above statement. However, notices once again the challenge of gathering quality data for quantitative assessments and the challenge to have an updated knowledge of the evolving cyber threat landscape.	Noted.
54	French Insurance Federation	Par. 1.27 - France assureurs agrees with the above statement. However, notices once again the challenge of gathering quality data for quantitative assessments and the challenge to have an updated knowledge of the evolving cyber threat landscape.	Noted.
55	French Insurance Federation	Par. 1.28 - The insurance industry would like to clarify that an ORSA is a company's own analysis and should remain that way. It is important to stress that the structure of the ORSA reports should be tailored to best present a company's risk profile and to provide the administrative, management or supervisory body (AMSB) and other interested parties with useful forward-looking analyses to define the company strategy. Therefore, the decision on how to perform the analysis on cyber risks in the ORSA in practice should remain at the discretion of the specific insurer. This includes the ORSA structure and concerned NCAs should therefore neither impose constraints nor prescribe an ORSA structure.	Disagree. EIOPA believes that if undertakings deem cyber risk as a material component of the overall retained exposures, this should be taken into account also in the ORSA evaluations. Also, considering the potential of non-affirmative cyber, addressing why the risk is not material is also in line with the aim of the ORSA. This

No	Stakeholder	Response to the public consultation	EIOPA's comments
		Furthermore, France Assureurs considers that no requirements to explain why a cyber risk is or is not material should be introduced. This does not exist for any other risk and would be inconsistent with general ORSA requirements.	is left open, in the full spirit of the ORSA, to the undertaking to evaluate.
56	French Insurance Federation	Question 1 - France Assureurs has been working with its members on the non-affirmative cyber risk since 2018. Different initiatives have been taken in order to have better visibility on the articulation of the guarantees mobilized to cover this risk (Club des juristes « Insuring cyber risks » Volume 1 [https://www.leclubdesjuristes.com/wpcontent/uploads/2018/01/cdj_rapport_cyber-risk_janvier-2018_uk_web.pdf] 2018, p.73). After a first step consisting in examining their exposure to non-affirmative cyber risk as a key element of their internal risk management process, insurance companies are taking action to address non affirmative cyber risk in casualty and property policies in order to comply with prudential requirements as well as in line with national supervisory recommendations in that regard. At the national association level, France assureurs is working on a mapping of the different solutions that companies are setting up to address their silent covers. France Assureurs would like to stress that our NSA (ACPR) issued in 2019, a press release regarding cyber risks coverage; with this document, the ACPR points out different areas of improvement for insurance undertakings regarding cyber-risks exposure (ACPR, Press Release « The distribution of guarantees against cyber risks by insurers », [https://acpr.banque-france.fr/sites/default/files/medias/documents/20191112_cp_bilan_cyber_assurance.pdf], 201). Insurers and reinsurers are also working together to strengthen their policies. Considering these initiatives (professional or supervisory) we are in the opinion that there is not a special need for an EIOPA action to address this issue.	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
57	French Insurance Federation	Question 2 - It is very difficult to understand the impact of a cyber event on guarantees covered by property and liability contracts. Hence, the main challenges for insurers to address and manage non-affirmative cyber risks are the capacity to have: - The expertise dedicated to cyber risks - The adapted and pertinent vocabulary to define as clearly and precisely as possible the terms related to cyber risks - The ability to be updated regarding the constantly evolving cyber threat landscape.	Noted.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		In terms of opportunities, addressing, managing and reducing exposure to non-affirmative cyber risks may result in a capacity for insurers to control their commitments by measuring their exposure (property, casualty, cyber), to align, monitor and adjust pricing and capital consideration regarding the overall cyber risk exposure to ensure compliance with undertaking's risk appetite. Moreover, the control gained on these guaranties allows insurers to better explain them to intermediaries and policyholders.	
58	French Insurance Federation	Question 3 - Adjustment of procedures and activities should occur at different domains: Claims (trainings, proposition, response plan, CAT plans), Accumulation Management (scenario definitions, data acquisition, cyber modelling update), Governance and Assurance (guidelines, external tools hands-on, cyber assessment framework) and Risk Engineers (Technical Standard for Cyber Exposure Review, Technical Standard Risk Grading for Cyber Security, Cyber Self-risk assessment tools). Cost estimation depends on the maturity and size of the company and should be replaced by a list of activities.	Agree. These principles are at higher level also conveyed through the messages provided in the Supervisory Statement.
59	French Insurance Federation	Question 4 - Reducing exposure to non-affirmative cyber risk through a better understanding of the risk may free up capacity on the market for writing affirmative cyber risk. However, challenges linked to the insurability of cyber risk are likely to remain, for example the high accumulation potential, the growing frequency and severity of cyber incidents, and the rate at which the threat landscape is evolving.	While EIOPA agrees on the topic of insurability, it also believes that further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand, thus ultimately generating request for increased capacity.
60	French Insurance Federation	Question 5 - Qualitative analysis is primarily used to measure exposure to non-affirmative cyber risk, however quantitative risk management methods are evolving. Improving access to quality data would help in further developing quantitative methods of analysis.	Noted.
61	French Insurance Federation	Additional Comments - France Assureurs is in the opinion that there is no specific need on this issue because, as expressed above, our NSA and our members are fully aware of issues arising from non-affirmative cyber-risks; if an action is nevertheless taken at EIOPA level, we would be in favour of the approach proposed under Policy Option 2.1 (Development of high	Noted. EIOPA believes that a Supervisory Statement provides the required flexibility and does not translate into a prescriptive rule-based policy action.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		level principle provisions which are less prescriptive and more flexible). High-level guidance on managing non-affirmative cyber exposures should provide the necessary flexibility to the industry to continue adapting underwriting practices to the constantly evolving cyber threat landscape and to continue adapting underwriting practices to the different natures of insured's activities. The issuance of more prescriptive rule-based policy action poses the risks of hampering the innovation which is necessary facing such an evolving risk.	
62	Insurance Broker Romania	Par. 1.5 - True	Noted.
63	Insurance Broker Romania	Par. 1.6 - True	Noted.
64	Insurance Broker Romania	Par. 1.8 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
65	Insurance Broker Romania	Par. 1.9 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
66	Insurance Broker Romania	Par. 1.10 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
67	Insurance Broker Romania	Par. 1.11 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
68	Insurance Broker Romania	Par. 1.12 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
69	Insurance Broker Romania	Par. 1.13 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
70	Insurance Broker Romania	Par. 1.14 - mandatory cyber insurance for EU	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
71	Insurance Broker Romania	Question 1 - mandatory cyber insurance for EU no feedback from Romanian parliament	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.

No	Stakeholder	Response to the public consultation	EIOPA's comments
72	Insurance Broker Romania	Question 2 - communication with IT people	Agree. This message was included in the Supervisory Statement in form of transversal cooperation across units within undertakings.
73	Insurance Broker Romania	Question 3 - N/a because it s beginning	Noted.
74	Insurance Broker Romania	Question 4 - yes	Noted.
75	Insurance Broker Romania	Question 5 - not relevant. cyber losses are dynamic trend for Increase monthly	Noted.
76	Insurance Broker Romania	Additional Comments - I M PRO BONO VOLUNTEER TO BE INVOLVED IN MANDATORY CYBER COVER	Noted. Establishing a mandatory scheme for cyber insurance in the EU is out of the scope of the Supervisory Statement.
77	Insurance Europe	Par. 1.5 - The frequency and sophistication of cyber incidents across all sectors has increased substantially, however this is due in large part to the rise of the Ransomware as a Service (RaaS) business model. While Covid-19 accelerated society's reliance on digital infrastructure, with opportune cyber criminals conducting pandemic-related phishing campaigns, it has also had a positive effect on the level of cyber awareness across society as a whole.	Agree. A footnote regarding this has been added to the text.
78	Insurance Europe	Par. 1.6 - Russia's invasion of Ukraine has most certainly contributed to the environment of instability around the world. However, this environment of instability in cyberspace is not new, nor related specifically to the war, as state-linked cyber criminals from Russia and other countries have been engaged in hostile activity in cyberspace for many years. Furthermore, while industries remain on high alert, the expected steep increase in malicious cyber activity linked to the war has so far not materialised.	Agree. A sentence of clarification regarding this topic has been added to the paragraph.
79	Insurance Europe	Par. 1.7 - The (re)insurance sector has a role to play in increasing awareness of cyber risk and promoting sound risk management measures among prospective insureds. The sector is part of many initiatives to raise awareness of cyber risks, which is fundamental to increasing resilience. For entities seeking to increase their resilience, cyber insurance can be part of the solution. However, risk management begins at the level of the entity, and insurers usually expect entities to take control over their exposures and implement a checklist of minimum cybersecurity measures as a precondition for purchasing cyber insurance. Cyber insurance should be seen as only one of a range of tools available for retail and corporate clients to use in increasing their cyber resilience, complementing the measures implemented at the level of the entity.	Agree. This messages are also conveyed thought the Supervisory Statement. A footnote has been added to further clarify the topic.

No	Stakeholder	Response to the public consultation	EIOPA's comments
80	Insurance Europe	Par. 1.8 - Cyber risk exposures are indeed under increasing scrutiny due to potential ambiguous terms and conditions in some policies. However, the sentence beginning "In fact…" should be amended in light of the following points: • "Affirmative cyber insurance policies" is a redundant term given that, by definition, a cyber policy affirmatively covers cyber risk. The word "affirmative" could be replaced by the word "dedicated". • The sentence "affirmative cyber insurance policies or cyber endorsements" implies that a cyber endorsement is not an affirmative cyber policy, which is incorrect.	No change. EIOPA believes that the definitions provided better fit for the purpose and follow commonly-used terminology.
81	Insurance Europe	Par. 1.9 - Cyber events can lead to potentially significant and unexpected losses in non-affirmative cyber exposures. Therefore, it is vital for undertakings to be aware of those risks and take them into account in risk management and calculation. Non-affirmative cyber exposure do not necessarily lead to higher uncertainty in claims settlement, and in most cases the opposite is the case. Non-affirmative cyber claims occur when coverage is granted independently of the triggering event (fire, third party claims, ...). This is usually easier to determine than the question of whether a specific cyber event triggered the damage.	Agree. This is in line with the overall messages conveyed by the Supervisory Statement.
82	Insurance Europe	Par. 1.10 - The treatment of war risk in cyber insurance policies is under increased scrutiny, particularly in light of current events. Discussions are ongoing in some markets to update traditional war exclusions to accommodate war of a cyber nature, for example in FR, where the Haut Comité Juridique de la Place financière de Paris (HCJP) recommended updating the legal definition of war risk to accommodate cyber warfare. Work has also been carried out by the Geneva Association in the area of attribution, where a new term 'Hostile Cyber Activity' has been coined to sit between cyber terrorism and cyber war, with the intention that, going forward, such a term may assist in distinguishing between what is insurable and what is not.	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
83	Insurance Europe	Par. 1.11 - Undertakings and supervisory authorities should be aware of and pay attention to risks that arise from nonaffirmative cyber exposure. However, since there are only a few known cases in Europe of claims covered by non-affirmative cyber coverage, this issue does not require high attention, and high-level guidance from EIOPA should be adequate to ensure convergence on this issue across the EU.	Noted. EIOPA believes that the issue of this Statement delivers the right answer to the current problems and will continue to monitor the market.

No	Stakeholder	Response to the public consultation	EIOPA's comments
84	Insurance Europe	Par. 1.12 - While the reference to the 2020 work is understandable as a step leading to the present statement, it is worth noting that the perception and handling of non-affirmative cyber exposures have strongly increased in the market in the past two years.	Agree. EIOPA welcomes the initiatives undertaken by the market and believes that the Supervisory Statement should give further help in achieving further results and let the industry move forward.
85	Insurance Europe	Par. 1.19 - Given that the EU already operates a comprehensive framework governing the terms and conditions reviews and policyholder communications, this Supervisory Statement should not result in any duplicative requirements, but rather utilise existing mechanisms.	Intentionally the statement only provides high level principles.
86	Insurance Europe	Par. 1.21 - The development of common terminology on cyber risks to be shared between (re)insurers, brokers and policyholders is an important area to be explored. Challenges associated with gathering quality data should also be considered, with assessment questionnaires that are supplied to/received from brokers amended and/or supported by external assessment tools.	Agree. This is in line with the message conveyed by the Supervisory Statement.
87	Insurance Europe	Par. 1.24 - Paragraph 1.24 relates to dedicated cyber insurance products, however the supervisory statement aims at non-affirmative cyber exposures. The point should therefore be deleted.	Although this Supervisory Statement does not cover neither overall management of affirmative cyber exposures, nor focuses on management of exclusions only, the link between those areas is structural and inevitable to enhance identification and management of non-affirmative cyber exposures.
88	Insurance Europe	Par. 1.26 - Insurance Europe agrees with the above statement however notes once again the challenge of gathering quality data for quantitative assessments.	Noted.
89	Insurance Europe	Par. 1.27 - The supervisory statement should refrain from referring to specific reinsurance structures as examples to the industry as this might imply that one kind of reinsurance structure is more suitable than another. The reference to "excess of loss covers or other non-proportional reinsurance arrangements" should therefore be deleted. In cyber, the only existing non-proportional covers are stop-loss (or their equivalent aggregate excess-loss). As regards the last sentence, in general, (re)insurers ask that primary insurers only cede affirmative risk, as reinsurance structures are generally not designed to cover non-affirmative exposures.	Noted. Reference to the quoted examples on the reinsurance treaty types has been removed.

No	Stakeholder	Response to the public consultation	EIOPA's comments
90	Insurance Europe	Par. 1.28 - Insurance Europe notes that the own risk and solvency assessment (ORSA) remains an individual assessment on the part of each company. As such, the incorporation of cyber risks into this analysis should remain at the discretion of the company.	EIOPA believes that if undertakings deem cyber risk as a material component of the overall retained exposures, this should be taken into account also in the ORSA evaluations. Also, considering the potential of non-affirmative cyber, addressing why the risk is not material is also in line with the aim of the ORSA. This is left open, in the full spirit of the ORSA, to the undertaking to evaluate.
91	Insurance Europe	Question 1 - Companies are continuing to examine their exposure to non-affirmative cyber risk as a key element of their internal risk management process, both to comply with prudential requirements as well as in line with national supervisory recommendations in that regard. In some markets, initiatives are ongoing at association level to examine the coverage provided by cyber policies and compare the policy wording with the intended coverage. In other markets, non-binding model clauses for cyber policies have been developed, where possible, and/or are in the process of being renewed. In DE, non-binding model clauses have been developed to affirmatively exclude or include cyber and blackout events from marine and transport insurance policies. In the UK, Lloyd's mandated in 2019 that all policies either affirm cyber coverage in, or exclude it from (re) insurance policies. This change was implemented using a phased approach with the fourth and final stage completed in July 2021. Lloyd's work is consistent with the approach taken by the PRA, which published a Supervisory Statement in 2017 on the cyber insurance underwriting risk to require Solvency II firms to robustly assess and actively manage their insurance products with specific consideration to non-affirmative cyber risk exposures. Firms are expected to introduce measures that reduce the unintended exposure to this risk through various mechanisms, such as introducing wording exclusions, premium adjustments and cover limits. In FR, France Assureurs is working on a mapping of different approaches that companies are taking to address their non-affirmative cyber cover. This follows a press release issued by the ACPR in 2019 highlighting areas of improvement for companies in tackling silent cyber risk.	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
92	Insurance Europe	Question 2 - In term of challenges, addressing and managing non-affirmative cyber risk requires the expertise of dedicated cyber risk engineers. Where less resources are available, underwriters must undertake specialised training and certification courses. External vendors	Noted.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		offer automated security perimeter evaluations that can help to identify a company's cyber exposure, however all of these trainings and resources come with significant costs. Additional challenges may arise due to the constantly evolving threat landscape and the need for terminology on cyber risks to be updated accordingly. In terms of opportunities, addressing, managing and reducing exposure to non-affirmative cyber risk may result in an increase in available capacity to offer affirmative cyber risk coverage. This may present an opportunity for growth in the cyber insurance market, notwithstanding the fact that significant challenges linked to the insurability of the risk are likely to remain (see Q4). In markets where policies generally do not contain exclusions for cyber risks, reducing non-affirmative cyber risk may lead to a growth in the number of cyber endorsements to traditional policies (property, liability).	
93	Insurance Europe	Question 3 - A cyber training course such as the ISC2 CISSP (Certified Information Systems Security Professional) is estimated to cost EUR 5000 per employee. This price includes the course and exam fees however it does not include the hidden cost of preparation time, estimated at around 70 hours. Adjustment of procedures and activities should occur at different domains: Claims (trainings, proposition, response plan, CAT plans), Accumulation Management (scenario definitions, data acquisition, cyber modelling update), Governance and Assurance (guidelines, external tools hands-on, cyber assessment framework) and Risk Engineers (Technical Standard for Cyber Exposure Review, Technical Standard Risk Grading for Cyber Security, Cyber Self-risk assessment tools). Cost estimation depends on the maturity and size of the company and should be replaced by a list of activities, whether general (claims, accumulation management) or cyber-specific (implementation of a next-generation antivirus, subscription to a Security Operations Centre).	Noted. EIOPA welcomes the price estimation provided.
94	Insurance Europe	Question 4 - Reducing exposure to non-affirmative cyber risk through a better understanding of the risk may free up capacity on the market for writing affirmative cyber risk. However, challenges linked to the insurability of cyber risk are likely to remain, for example the high accumulation potential and the rate at which the threat landscape is evolving.	While EIOPA agrees on the topic of insurability, it also believes that further clarity in exposures and policy wording might result in clearer information provided to the demand side and therefore increased demand from potential policyholders. With an increase in demand, supply would then move into the direction of reaching the natural equilibrium between supply and demand,

No	Stakeholder	Response to the public consultation	EIOPA's comments
			thus ultimately generating request for increased capacity.
95	Insurance Europe	Question 5 - Qualitative analysis is primarily used to measure exposure to non-affirmative cyber risk, however quantitative risk management methods are evolving. Improving access to quality data would help to further develop quantitative methods of analysis. In DE, the GDV established a monitoring system for non-affirmative cyber claims to help undertakings to understand and quantify the relevance of non-affirmative cyber risks.	Noted. EIOPA welcomes the development of such initiatives and encourages the sharing of good practices.
96	Insurance Europe	Additional Comments - As a general remark, it is worth noting that while EIOPA has titled its statement "management of nonaffirmative cyber exposures", the content of the statement goes beyond this theme, addressing entities' management of cyber risk as a whole. Insurance Europe agrees with the approach proposed under Policy Option 2.1 (Development of high level principle provisions which are less prescriptive and more flexible). High-level guidance on managing nonaffirmative cyber exposures should provide the necessary flexibility to the industry to continue adapting underwriting practices to the constantly evolving cyber threat landscape. Certain terminology/wording used in the statement would benefit from clarification: • There is a difference between desired non-affirmative exposures (for instance in property policies the cyber-induced fire and explosions, also called inherent silent) and undesired exposures (non-damage BI following a cyber attack, also called residual cyber). • Similarly, under policy options, the paper refers to "accumulation of non-affirmative cyber risk and systemic risk resulting from cyber incidents". Insurance Europe seeks clarity on the wording as it could be implied that systemic risk emerges from affirmative cyber risk only.	Although this Supervisory Statement does not cover neither overall management of affirmative cyber exposures, nor focuses on management of exclusions only, the link between those areas is structural and inevitable to enhance identification and management of non-affirmative cyber exposures. A clarification sentence has been added to the introductory paragraphs to the Supervisory Statement.
97	Unipol Gruppo S.p.A.	Par. 1.11 - Whereas we agree with EIOPA's statement, we would like to highlight that the issue of non-affirmative cyber exposure is now becoming of less and less importance by virtue of the actions already undertaken by the insurance companies, especially in relation to the new contracts. Indeed, in the past years many insurance companies have already performed some kind of review of non-affirmative cyber-risks on their non-life policies and included explicit exclusions in their new products, also to meet the clients' expectations towards more clarity on the scope of the insurance protection. The residual non-affirmative cyber risk often stems from legacy contracts (10+ years) and does not reach a materiality threshold for many undertakings.	EIOPA believes the management of non-affirmative cyber exposures cover a paramount role in the development of a sound market for cyber insurance. Furthermore, EIOPA welcomes the work on exclusions done so far, but advises to perform continuous wording reviews to keep up with the speed of the risk evolution, the consumers' demand and to

No	Stakeholder	Response to the public consultation	EIOPA's comments
			the overall benefit of the risk management framework.
98	Unipol Gruppo S.p.A.	Par. 1.18 - Although we agree with EIOPA's recommendations, we deem necessary to re-inforce the principle that such supervisory expectations shall be calibrated on a proportional and risk-based approach. In particular, cyber risk exposure does not reach a materiality threshold for many insurance undertakings and, thus, including this specific risk into the whole ORSA process may prove an unduly burdensome exercise. Also, looking forward, an endless widening of the scope of the risks fully taken into account in the ORSA risks being unbearable for insurance undertakings. Therefore, suggestion is rewording par. 1.18 as follows: "NCAs should ensure that – subject to a materiality assessment and according to a risk-based approach – (re) insurance undertakings [….]".	Agree. Paragraph has been redrafted according to the suggestion proposed.
99	Unipol Gruppo S.p.A.	Par. 1.21 - When developing risk quantification models, insurers face three kinds of challenges: (i) lack of data; (ii) methodological limitations and (iii) correlated risks. As to the lack of data, it is worth noting that insurance companies have an average of 10 years of cyber insurance claims data available to support underwriting and modelling, compared to more than one hundred years' worth of data to assess potential losses from other perils. In addition, detection and discovery rate are low for cyber incidents and most firms prefer not to disclose cyber security breaches, if they have the opportunity to do so. As to the methodological limitations, scholars have pointed out that ever-changing threats from intelligent adversaries differentiate cyber risk from other perils as it denies insurance companies the kind of historical patterns they rely on to properly assess risks. Furthermore, the fact that the cyber space is interconnected and attacks can easily be performed on a large scale complicates significantly the loss modelling. Therefore, we propose to reword the provision of par. 1.21(a) in a less prescriptive way, e.g. "specific and reasonable efforts should be made […]". In addition, it is worth considering that monitoring cyber risk exposure is a complex and costly exercise and, thus, it should be performed according to a risk-based approach. In particular, insurance undertakings that have assessed material cyber exposures should be monitoring cyber risks and reviewing their contracts on a more frequent basis compared to those entities whose cyber underwriting exposures do not meet a materiality threshold. Thus, suggestion is rewording paragraph 1.21 as follows: "[…] consistent with a risk based approach and the overall business strategy set by the AMSB […]".	EIOPA believes that the lack of data is only one part of the picture, but also believes that good management of non-affirmative cyber exposures should lead to clearer exposures definitions and therefore allow application of more sophisticated quantitative models.
100	Unipol Gruppo S.p.A.	Par. 1.22 - On a general note, we agree that traditional war and terrorism exclusions can lead to legal disputes and reputational risks for insurance undertakings, also due to uncertainties related to the legal definition of "act of war". However, even though international laws do	Noted. A footnote mentioning some of the references provided has been added.

No	Stakeholder	Response to the public consultation	EIOPA's comments
		not define the "act of war" with regard to cyber-space, it is worth considering that scholars, court cases and diplomatic initiatives support the conclusion that even the use of a "cyber weapon" as a computer can constitute unlawful use of force and/or an armed attack (see, amongst others, the Tallinn Manual on the International Law Applicable to Cyber Operations and the Cyber Diplomacy Toolbox developed by the EU ministries of foreign affairs in 2017, which states that "existing international law is applicable to cyberspace"). That being said, many scholars believe that there is strong case arguing that States should take responsibility for protecting civilians from losses resulting from state-sponsored cyber-attacks, especially when those are widespread and surpass a materiality threshold in terms of harmful consequences. In this respect, the Tallin Manual proposes that a cyber-attack shall be deemed as an "attack" under international law when it is "reasonably expected to cause injury or death to person or damage or destruction to objects". In this respect and also in light of the limited insurers capacity to bear losses, we deem inevitable that certain extreme cyber events will be excluded from coverage by the whole industry.	
101	Unipol Gruppo S.p.A.	Par. 1.26 - As to the quantification of cyber risk exposure and the related obstacles to the development of complete and accurate models, please refer to our comment to par. 1.21.	Noted.
102	Unipol Gruppo S.p.A.	Par. 1.27 - We do not agree with the proposed approach, considering that an explicit regulatory recommendation to rely on reinsurance treaties to bear large cyber events could trigger unintended market consequences in terms of soaring prices and depletion of the overall reinsurance capacity. In addition, it does not seems appropriate recommending together a reinsurance cover for both affirmative and non-affirmative exposures. Indeed, coverage of non-affirmative cyber exposure entails a costly due diligence process by the reinsurers that may prove unworthy for most insurance undertakings with non-material risk exposures. In light of the above, we deem appropriate rewording the whole par. 1.27 replacing the explicit recommendation "to make use of" reinsurance capacity with that of "assessing the opportunity to make use of", which would be more proportionate and would avoid the abovementioned unintended consequences.	Noted. The paragraph has been redrafted according to the suggestion.