Prepare and Prevent, Don't Repair and Repent

The Role of Reinsurance in Offensive Cyber

Alicia Bates

ABSTRACT

Insurance is often treated purely as a tool to mitigate financial risk. The insured can pay a premium for the confidence that if a cyber-attack occurs, they are indemnified for their losses. This paper advocates that insurance can play a more significant role dealing with offensive cyber, by way of relying upon a reinsurance framework. An appropriate insurance framework which assists a non-state actor before, during, and after an attack can facilitate a coordinated response to supporting a state's national security objectives. When a state opts to use an offensive cyber operation, there is a risk that the operation will inflict unintended consequences/harms and will trigger a retaliatory attack. The proposed reinsurance framework would assist in improving a business's resilience and security. An underlying reinsurance regime will ensure the framework transfers risk from a specific business and spreads it across society. This paper argues that by reducing and responding to risks and unintended consequences of offensive cyber operations with reinsurance, a state's offensive cyber strategy may receive a more favourable reception from society. This reduces the risk that an offensive cyber strategy may delegitimise the state.

INTRODUCTION

Defensive cyber operations have traditionally dominated state responses to attacks upon domestic-based networks.[1] However, there is an increasing shift towards states choosing to use offensive cyber operations against other states and non-state actors.[2] While a set definition does not exist in the literature, offensive cyber strategies could involve a state "pursuing or disrupting cybercrime, conducting digital counterintelligence, or military cyber operations."[3] The trend of favouring offensive

Alicia Bates is a Senior Tutor at the University of Law where she teaches international commercial law. Alicia is currently studying for her Ph.D. at King's College London under the supervision of Professor Özlem Gurses and Dr. Tim Stevens. Her Ph.D. is entitled: 'Terrorism: when, not if. Time to insure the uninsurable risk? *An intensive investigation into the legal framework governing mandatory insurance*.' Alicia's research interests lie in insurance, terrorism, and cyber. Prior to undertaking her Ph.D., Alicia was called to the Bar of England and Wales by the Honourable Society of the Middle Temple where she was awarded the Harmsworth Scholarship and the Hong Kong Scholarship. Alicia has also taught at BPP University and taught insurance law as a visiting lecturer at King's College London. Alicia is a Fellow of the Higher Education Academy.

cyber operations raises two issues for states. First, how should the state respond to the risk that foreign states might use an offensive cyber strategy against them or domestic non-state actors? Second, what are the risks of a foreign state retaliating against a state that has deployed an offensive cyber strategy? The issue of attribution is concomitant with both of these questions. Offensive cyber operations are typically classified. This presents practical and legal issues of how a state, or insurer, investigates and attributes an attack.

When a state uses an offensive cyber strategy, there is a risk that the operation will result in a foreign state retaliating.[4] This retaliation could harm the state or non-state actors. This paper suggests that an insurance framework, which is underpinned by reinsurance, and assists a business before, during and after an attack, could improve the resilience and security of domestic businesses in response to cyber attacks. This increase in resilience and security, coupled with the spread of risk by way of reinsurance, would support a state's national security objectives when their strategy involves offensive cyber operations.

Insurance companies can enlist a cyber expert to assess a business's cyber security prior to the insurance contract being drafted. The insurer can impose contractual obligations upon the insured to ensure that some or all of the expert's recommendations to improve their cyber security are implemented before the commencement of the insurance policy. This contractual protection mitigates the insurer's scope for liability. Insurance companies could hire a team of cyber experts who are on-hand to assist an insured during an attack. Having immediate help will limit the impact of the attack. This is not only beneficial to the insured, who will be more likely to experience fewer losses, but also the insurer who will, consequently, have to pay out less to the insured.

The author anticipates the insurance industry would not receive her proposals favourably unless an adequate state-based reinsurance framework underpinned the proposals. State-based reinsurance would assist insurance companies meet their liabilities to the insured once a claim was over a certain financial amount.[5] This would ensure that insurers were able to withstand the potential implications of a state's offensive cyber operations. Reinsurance would spread the risk of a cyberattack across society. The transfer and spread of risk from an insured business to society as a whole, will provide greater flexibility for the deployment of a state's national security objectives. The mitigation of loss arising from an insurer's assistance in improving resilience and security prior, during and after attack is important to ensure the underpinning reinsurance regime remains financially viable. The pre-emptive establishment of reinsurance, underpinned by a state guarantee, allows a state to acknowledge that their strategies may cause direct or indirect harm to domestic non-state actors.

While this paper addresses reinsurance in the UK, it is important to note that the ideas in this paper could easily be extrapolated and relied upon by many states across the globe, such as the US. The idea in the paper could see a broader move by states to support the resilience of domestic companies through reinsurance. This could improve perceptions of a state's offensive cyber strategies. This proposed insurance framework may appear to be defensive in nature and to some extent it is. However, insurance can enable a good defence against offensive cyber strategies. By improving this defence, it supports a state's national security objectives.

Part I: The Scope for Harm Emanating from Offensive Cyber Strategies

Insurance is a risk management tool.[6] Insurance contractually divides a specific risk between the policy holder (the insured) and an insurance company (the insurer). In recent years, the market has pushed for indemnity insurance to be offered to cover cyber-attacks. The WannaCry cyber-attack exemplifies why insurance is sought by the market. Within 24 hours, 230,000 computers in around 150 countries had been affected.[7] This affected governmental organisations and businesses alike. The National Health Service (NHS) saw a third of trusts across the UK affected because of infected and locked out devices and consequential cancelled appointments.[8] Beyond the practical impact, WannaCry also had a fiscal impact on the NHS. Kristensen et al found that "[t]he total economic value of the lower activity at the infected trusts during this time was £5.9m including £4m in lost inpatient admissions, £0.6m from lost A&E activity, and £1.3m from cancelled outpatient appointments."[9] Had a kill switch not been found on the same day as the WannaCry attack, one can foresee how these losses could have been greater. It is estimated that if the attack had affected all trusts, the loss in activity alone could have reached up to £35m.[10] While this attack was not a target arising from the UK's offensive cyber operations, it is a clear example of how a foreign state's attack on part of the UK's critical infrastructure could cause considerable financial harm and disruption.

The attack on SolarWinds helps to further contextualise how cyber attacks can induce retaliatory attacks. SolarWinds is a US information technology firm which attracts high profile

clients such as Fortune 500 companies and government agencies.[11] In March 2020, SolarWinds sent updates of their software to 33,000 customers (around 18,000 customers installed the update). This update included a malicious code which allowed the hackers to access sensitive customer information and install malware to spy on customer systems. The level of sophistication of the attack meant that it went undetected for months and to date, many customers do not know if they were a victim of the attack.[12] It is believed that the malicious code was directed by the Russian intelligence service. The attack resulted in President Biden imposing sanctions against Russia. When deciding to employ these sanctions, President Biden will no doubt have been live to the possibility that Russia could retaliate. This raises the question of how can a state ensure that their domestic defence is able to withstand retaliatory effects from an offensive cyber strategy?

Beyond the fiscal impact of an attack arising from business interruption, an insured can face other losses; for example, the insured may become liable for breaches of confidentiality to third parties or a loss in reputation. The CEO of Lloyd's London, Inga Beale, argues that "[t]he reputational fallout from a cyber breach is what kills modern businesses. And in a world where the threat from cybercrime is when, not if, the idea of simply hoping it won't happen to you, isn't tenable."[13] This reputational impact can occur because an assailant can access a great deal of confidential information which, if leaked, could cause significant harm to many of the companies associated with the target company.

An example of this is the Hafnium attack on Microsoft. The Hafnium attack involved a group attributed as a Chinese state-sponsored actor. The group exploited vulnerabilities with Microsoft's Exchange Server. While estimates differ greatly, it is estimated that this attack impacted anywhere between 10,000 and 250,000 of Microsoft's customers, including businesses, governmental agencies, and schools.[14] It is possible that these customers will have developed negative perceptions of Microsoft as a result of the impact on Microsoft's Exchange software. This might have resulted in those customers looking to Microsoft's competitors for the provision of email software. This shift in customer behaviour would likely harm Microsoft's profit margins. However, beyond this, the Hafnium attack demonstrates that there are positive externalities for strong defence against cyber operations, an attack on one company can harm other actors, such as businesses within the supply chain of the target business. With relations between the US and China continually being challenged, the scope for either state to retaliate and use cyber offensive strategies in response to Hafnium is foreseeable.

The attacks cited highlight the level of risk that can be attributed to cyber-attacks. With the continuous evolution of technology and growing willingness of states to use offensive cyber capabilities, one might argue that the scope for harm transcending quantifiable losses could only continue to evolve. Thus, it is important to ask: how can reinsurance assist in allowing the role of insurance to evolve and move beyond simply indemnifying an insured's losses arising from an offensive cyber operation?[15]

Part II: Improving a Non-State Actor's Resilience Before an Attack

The premium paid by the insured to the insurer represents the cost of the risk covered by the policy.[16] This is termed the "actuarially justified premium."[17] If the premium is too low and a loss is realized, an insurer could become insolvent fulfilling its liability to the insured. Premiums are therefore set at a rate to create a sufficiently large capital to ensure considerable losses can be covered. While many economic models have been developed regarding cyber risk estimation and premiums,[18] it is worthwhile asking: what if this premium could cover a service beyond the promise of indemnifying future losses?

In English law, the insured must disclose any information which may affect the objective insurer's decision to insure. This disclosure will satisfy the insured's duty of fair presentation of the risk.[19] For example, the reasonably prudent insurer would likely want to know about a previously successful cyber-attack on the insured, as this would identify potential vulnerabilities in the insured's networks. However, the insured must only disclose information that they know or ought to know.[20] The difficulty is that many companies, understandably, lack knowledge about their cyber risk. This is prevalent in relation to risks emanating from offensive cyber operations as states rarely disclose the full detail of their operations for the purposes of national security. Thus, the disclosure obligations on the insured are fairly minimal; not least, because any information which is publicly available regarding the threat actor need not be disclosed by the insured to the insurer, as the insurer can be presumed to know the information.[21]

Cyber experts can assist companies in assessing and minimising their risk. While cyber experts are not going to be privy to a state's offensive cyber strategies, they will have an in-depth understanding of vulnerabilities with specific software and industries. However, these experts are expensive, and the cost is rising. In 2012, Caldwell Partners, an Executive Search Firm, paid $650,000 a year for a cyber expert to join on as Chief Information Security Officer. In 2019, that salary had risen to $2.5 million.[22] Bloomberg accounts this growth to the increase and severity of cyber-attacks, and also the fear of litigation and the associated fines.[23] Whilst many advisory firms are available to conduct cyber risk assessments, these are costly, and the cost is not going to decrease soon. This might mean that the cost of an expert is considered by the insured to be unaffordable or disproportionate to the perceived benefit. One way an expert could be used would be by conducting a risk assessment of the insured's business prior to the insurance policy being drafted. This risk assessment could be accompanied with recommendations for improvements. Although one might perceive this as expecting the insurance industry to provide a new and free service to the insured, the insurance industry will actually see reduced claims as a result of the increased resilience. Furthermore, insurers do already assess a client's risk either at the point of quotation or renewal. This risk assessment dictates the premium the insured will pay. The proposal therefore seeks to use the wealth of knowledge that advisory firms have and input it into the insurance coverage process in a standardized manner.

Used appropriately, this risk assessment could mean that insurance could be seen as a vital tool to improve a company's resilience and improve standards overall to reduce the impact of cyber operations by states. The anticipated cover would compensate the insured for losses arising from a foreign state's cyber operations. A definition clause in the policy would dictate that the policy would cover operations which have been attributed to a state directly, or a stated sponsored actor, as seen with Hafnium. There would be no requirement that the attack was in retaliation to the domestic state's cyber operations; any legal clause attempting to do so, would render the policy challenging to claim on owing to evidential issues, not least with attribution. Many offensive cyber strategies are subject to national security. This confidentiality means that proving an attack was in retaliation could be near impossible. That is not to say that attributing the attack which has caused losses will be straightforward. Although attacks such as SolarWinds and Hafnium have been attributed to state-sponsored actors, this took a considerable amount of time. The issue of attribution will need to be explored further and is worthy of discussion with academics across the field. However, it is worthwhile noting that the legal standard of attribution and the political standard is very different. This leads the author to believe that attribution is not an insurmountable obstacle for the proposed policy. As a matter of law, an insurer is liable where the loss was caused by an insured peril. Causation and loss must be established on the balance of probabilities; in other words, the loss was more likely than not a result of a foreign state's cyber offensive operations. For many states, this would be too low of a bar to explicitly attribute an attack to another state. Often states are tentative in their attribution, as they are mindful of the potential ramifications if their attribution is proved to be inaccurate. Thus, upon overcoming the challenges faced with attribution, one can foresee how the coverage may reassure a state that they can use a cyber offensive strategy, safe in the knowledge that they have an adequate defense, should retaliation occur.

Cyber experts can reflect upon previous attacks to assess a company's vulnerabilities and develop a system of best practices while responding to the specific company in question. These recommendations would then be assessed by the insurer, who could then decide whether the proposed improvements should remain voluntary for the insured or whether they ought to be incorporated as clauses into the insurance policy. These clauses could take two forms: a warranty or a condition precedent.

A warranty is a promise that the insured has done something (a present warranty) or will continue to do or not do something (a continuing warranty).[24] A warranty might confirm that a state of affairs is true, for example, that the insured has installed a firewall onto their computer systems. If this warranty is breached, the insurer's liability is suspended for the period of time that the insured has not complied with the warranty.[25] It should be noted that, save that it is a risk defining term, this suspension will only relieve the insurer of liability if the risk of the specific loss faced by the insured was materially affected by the breach.[26] For example, a failure to install a firewall would be unlikely to materially affect the insured's risk of their premises

flooding. However, as we are speaking about losses arising from a cyber attack, one can assume that the imposed warranties would materially bear on the losses the insured was seeking to cover insofar as offensive cyber operations are concerned and therefore might be regarded as a risk defining term. The scope for loss arising from a cyber attack would likely mean that most insureds would be motivated to ensure that they would be indemnified under the policy.

Alternatively, the insurer could impose a condition precedent on the insured. There are three types of condition precedent: to the policy, to the inception of the risk, and to the liability. A condition precedent to the liability is relevant to the claims making stage. A condition precedent to the policy means that the validity of the entire contract depends upon the insured's compliance with the condition precedent. Furthermore, a condition precedent to the inception of the risk means that while a contract exists between the insurer and the insured, there is no coverage of the risk unless there is compliance—in every practical sense, the contract is useless without compliance with the term. If the insurer is particularly interested in the insured taking specific steps prior to agreeing to indemnify the insured, these options would be more desirable for the insurer. An example might be that the insurer stipulates that an insured imposes a multi-factor authentication on all technological devices for all users. In this scenario, a condition precedent to the policy would mean that the policy would not be rendered valid until the authentication system was employed. Alternatively, a condition precedent to the inception of the risk would mean that, while the policy was valid, it would not cover the risk of cyber-attacks until the authentication system was active.

In summary, the insurer can provide a cyber expert to the insured as part of the insurance policy package. The cyber expert can identify the insured's vulnerabilities, which will then allow the insured to take proactive steps to minimize their risk and improve their resilience. The insurer can enhance this protection by including terms that require the insured to take the necessary steps to minimise their risk of loss. The insurer would be able to factor the inclusion of these clauses into their risk assessment, known in the insurance industry as the underwriting process.

Part III: Improving a Non-State Actor's Resilience and Security During and After a Cyber Attack

While the insured's risk can be mitigated by way of improving their resilience, one must accept that the risk a non-state actor will be harmed because of an offensive cyber strategy (be it indirectly or directly) cannot be eradicated. Because of this, it is pertinent to reflect upon how an insurer can assist the insured in ensuring that the losses arising from a cyber-attack are constrained as much as possible. This is a laudable goal. If the UK plans to use offensive cyber strategies, improving non-state actors' defences against a foreign non-state actor's retaliatory attack recognizes the potential consequences of the UK's actions. This is not only important for improving a non-state actor's resilience prior to an attack, but also their resilience and security during and after an attack. If state and non-state actors within the UK have a more robust defense

system and if the UK is forced to take a particularly extreme offensive cyber operation (such as disrupting the supply of a utility like electricity to an entire city or engaging in military conflict), the state and non-state actors within the UK will feel more confident in defending any retaliatory attacks. By using the proposed framework, the UK further demonstrates that its offensive cyber strategies are being used in a manner which is compatible with democratic governance.

One way to improve democratic governance is by ensuring there is accountability, oversight, and transparency within the government.[27] Oversight and transparency are not always achievable given the national security implications, the complexity of the associated networks and the associated expertise of oversight bodies, and the interplay between public and private cooperation.[28] In this regard, a focus upon accountability might facilitate the UK's use of offensive cyber strategies. As such, insurance could play an invaluable role in ensuring that any harm inadvertently imposed upon a non-state actor because of an offensive cyber strategy was compensated for accordingly. This is supported by Weber's approach towards the ethics of responsibility which suggests that a government should be mindful of pursuing a strategy which in the best interests of the nation.[29] While offensive cyber strategies may be entirely justified when someone is armed with the full information regarding the threat faced by the UK,[30] the government does still need sufficient support from society (who will likely be unaware of the extent of the threat) to ensure that their actions do not undermine the legitimacy of the government. The transfer and spreading of risk is one way insurance can assist in this regard. However, it is anticipated that the insurance industry would not view these proposals as favourable unless an adequate state-based reinsurance framework underpinned the proposals.

When the insurer has a team of cyber experts on hand, they can deploy the experts to the insured's premises as soon as they are notified that an attack is underway. This will particularly assist an insured who is victim of a retaliatory attack after a foreign state has engaged in offensive cyber strategy. It may be challenging to determine that the attack was as a result of an offensive cyber strategy at the point the insured realises an attack is taking place. This is not insurmountable. The insured will likely have multiple policies with the insurer which cover different types of risk. One policy may cover cyber attacks conducted by non-state actors, where the other covers state actors or state sponsored actors. This may be done under one comprehensive policy or under two separate insurance contracts. This article focuses upon offensive cyber and thus, further exploration of insurance cover must be limited. The author has produced research which considers how these policies can be used for cyber attacks more generally, and potentially for cyber terrorism, should it eventualise in the future. This highlights the potential scope for these policies to reshape the vast sectors of the insurance industry.

A cyber expert would be able to assist the insured in minimizing the harm and recovering from an attack as quickly as possible. We can consider the Hafnium attack on Microsoft as an example of how this could work in practice. The vulnerabilities in the software that led to the 0-day exploit have since been patched by Microsoft, but that software is used by many compa-

nies around the world. Cyber experts would be able to suggest how to address evolving threats by relying upon their knowledge developed from previous attacks in a way in which many non-state actors would be unable to do on their own.

Relying on a cyber-expert to assist would align with Woods and Böhme's research, which found current market practice dictates that when a policy holder suffers an incident, they call a hotline which puts together a team of responders to help the insured respond to the attack and minimize harm.[31] At the moment, insurers typically advertise a list of preferred or pre-approved cyber experts, having cyber experts on hand who could be deployed directly by the insurer as part of their insurance service would streamline the efficacy of the intervention.

To ensure the probability of successful intervention is as high as possible, the insured may consider introducing a condition precedent to the liability in the insurance policy. A condition precedent to the liability means that the insurer faces no liability unless the insured complies with the condition precedent at the claims making stage. For example, a condition precedent to the liability might require the insured to co-operate with the insurer in the period after the attack to ascertain the identity of the assailant. In the words of Longmore LJ in *Royal & Sun Alliance Insurance Plc v Dornoch Ltd*,[32] "a condition precedent to the liability of the reinsurer operates as an exemption to that prima facie liability."[33] If the insured failed to comply with the condition precedent and brings a claim for a loss, the claim will fail.[34] Thus, the insurer may wish to implement a claim provision which is a condition precedent to the liability and which stipulates that the insured must notify the insurer as soon as reasonably practical that an attack is underway. The insured could go further and introduce a time bar. For example, they could stipulate that the insured must notify the insurer within 3 hours of discovering the attack. The effect of failure to comply with such a condition precedent would mean that the insurer would not be liable for any losses arising from that specific cyber-attack.

It should be noted that a breach of this condition precedent does not invalidate the insurance policy and the insurer would remain liable for future claims, provided the insured complied with the clause on that occasion. This clause would also be important to safeguarding over-reliance upon a reinsurance regime. While the reinsurance regime further assists in developing state accountability, it is important that the regime remains fiscally viable. One way to ensure the reinsurance regime remains affordable is to mitigate the regime's use as far as possible.

Part IV: The Use of Reinsurance to Assist in Improving Domestic Resilience

Whilst the above discussion has highlighted how insurance companies can facilitate improving the defensive position of non-state actors in the UK, thereby supporting the UK's national security objectives, it is important to ensure this framework is financially viable for insurers. To do this, it is important to briefly consider how state-based reinsurance could supplement the framework. This paper argues that reinsurance would indicate a state's willingness to support insurance companies in improving domestic resilience. This is because state-based reinsurance

could assist insurers where large sums were owed to non-state actors because of losses directly or indirectly emanating from the UK's offensive cyber operations.[35]

Insurance companies are businesses, therefore, while their service is to indemnify an insured's loss, upon an insured peril occurring, it is vital that the service provided is sustainable for the insurer. If a proposed service becomes financially unviable for the insurer, the insured's risk increases further as there is a chance that the insurer will become insolvent before indemnifying the insured. This would be problematic not only for the insurer and the insured but society as a whole, as a result of systemic risk: businesses are heavily interconnected and if one goes insolvent, there could be a ricochet effect which destabilizes the economy of a state. It can be argued that attacks such as WannaCry and Hafnium both demonstrate that cyber attacks can not only result in particularly high financial claims but also that minimizing the harm caused by cyber attacks positively impacts society as a whole. This is particularly true if we consider the fact that insurers typically insure a vast array of risks. Therefore, their insolvency would not only impact businesses but anyone who held an insurance policy with that insurer. If the UK is planning to employ further offensive cyber operations, it is worthwhile to reflect upon the impact that will have on non-state actors and their insurers. This is where reinsurance comes in and acts as a facilitator to improve domestic resilience throughout the UK.

Reinsurance is where the government provides an insurance framework to insurers. While the UK has Pool Re as a reinsurance scheme available for terrorism, no such reinsurance scheme exists for cyber risk. Pool Re was established, in tandem with the insurance industry and Her Majesty's Treasury, to help insurance companies offer insurance coverage after a terrorist attack. Pool Re provides reinsurance in the event an insurer is unable to meet the claims after an attack. Rather than allow for a situation where the insurance market rejects policies for cyber risk, it would be more appropriate for the government to pre-empt this development as part of their National Resilience Strategy, supported by the National Cyber Security Centre. Thus, the pro-active approach would likely increase societal perceptions of the UK's offensive cyber strategy as it is indicative of not only governmental accountability, but also the forward looking nature of the UK's offensive cyber strategy.

One might raise the question why reinsurance alone would not be sufficient to support the existing cyber insurance framework. As previously stated, an insurer's liability can be reduced by minimizing a non-state actor's scope for harm by improving their resilience and security. This is important if one accepts the proposition that a state's increased use of offensive cyber strategies is likely to, in turn, increase non-state actors' risk of attack by a foreign state. By using the proposed insurance framework in tandem with a reinsurance framework, it ensures any reinsurance provided by the government remains viable long term. For example, reinsurance might only be available to the insurer once their liability exceeds a certain financial sum. While it remains prudent for the insurer to invest some of the premium received by the insured into hiring the most skilled cyber security experts to minimize their scope for liability,

it could be required that an insurer be able to benefit from the reinsurance scheme. This would ensure that a middle ground is found between state accountability and a realistically affordable framework.

CONCLUSION

As states continue to move towards using cyber offensive strategies, it is important to recognize the impact these strategies can have upon non-state actors. There are two points to consider in relation to the role of reinsurance with regards to offensive cyber operations.

First, by recognising the global trend towards states preferring offensive cyber strategies, it is important for the UK (and states across the globe) to improve their own defenses against a foreign state's use of offensive cyber operations. In this regard, insurers can transcend their classic indemnification role and evolve to providing a service that helps to prevent and mitigate the harm emanating from offensive cyber strategies thereby playing a key role in improving a non-state actor's security and resilience.

Second, when the UK uses an offensive cyber strategy, non-state actors can be indirectly and unintentionally harmed, not least if they become victim to retaliatory attacks. In this regard, a reinsurance framework, which spreads the risk from non-state actors across society will likely align with the UK's national security objectives. While a reinsurance regime plays an essential role in ensuring that the proposed framework is feasible for insurers, it is essential that the reinsurance regime is equally feasible long term. For this reason, it is important that insurance work towards improving the insured's resilience using pre-emptive cyber advice and integrating this into contractual obligations for the insured.

NOTES

1. S Bradbury, "The Developing Legal Framework for Defensive and Offensive Cyber Operations," *Harvard National Security Journal* 2, no. 2 (2011).
2. For example, the UK was the first to acknowledge that offensive cyber was a viable option, within the confines of international law, to respond to the risk of a cyber-attack see J Blitz, "UK becomes first state to admit to offensive cyber attack capability," *Financial Times*. 2013, https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de. Furthermore, the creation of the National Cyber Force in 2021 was intended to improve the UK's offensive cyber capabilities see "National Cyber Strategy 2022," UK Government, 2022, accessed 17th February, 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.
3. *The National Cyber Force that Britain Needs?* (Kings College London; Offensive Cyber Working Group, April 2021).
4. Although retaliation is not strictly permissible under Article 51 of the UN Charter, this does not mean that offensive cyber strategies cannot enter a grey area where the line between legitimate proportionate responses and unlawful retaliatory responses blur.
5. This financial amount would be determined by the state.
6. F Martin, *The History of Lloyd's and of Marine Insurance in Great Britain* (London: The Lawbook Exchange Ltd, 1876).
7. "Cyber-attack: Europol says it was unprecedented in scale," *BBC News* May 13, 2017, https://www.bbc.co.uk/news/world-europe-39907965.
8. W Smart, "Lessons learned review of the WannaCry Ransomware Cyber Attack," February 1, 2018.
9. S Kristensen, S Ghafur, K Honeyford, G Martin, A Darzi and P Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *npj Digital Medicine* 98, no. 12 (2019).
19. Ibid.
11. "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal," Business Insider, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T.
12. D Volz and R McMillan, "Hack Suggests New Scope, Sophistication for Cyberattacks," 2020, https://www.wsj.com/articles/hack-suggests-new-scope-sophistication-for-cyberattacks-11608251360; "The SolarWinds Cyber-Attack: What You Need to Know," 2021, accessed March 15, 2022, https://www.cisecurity.org/solarwinds.
13. "Closing the gap. Insuring your business against evolving cyber threats," 2017, accessed 30th October 2021, https://assets.lloyds.com/assets/pdf-lloyds-cyber-closing-the-gap-full-report-final/1/pdf-lloyds-cyber-closing-the-gap-full-report-final.pdf.
14. R McMillan and D Volz, "China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers," *The Wall Street Journal* 2021, https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991?mod=tech_lead_pos1.
15. It should be noted that some insurers may already play a role in improving a business' security and resilience. For example, insurers may pay for the expenses incurred to prevent or minimise the insured loss. The insured might prevent a loss and might claim the expenses incurred for that purpose from the insurer. Moreover, insurers generally ask the assured to take risk mitigation precautions. As such, whilst the proposals in Part II and III demonstrate how the insurance industry might move their collective practices to assist offensive cyber operations, the main focus of this paper is on how a state-based reinsurance scheme can help develop the insurance industry's facilitation of improving domestic defence in anticipation of a retaliatory attack after an offensive cyber strategy.
16. F Ewald, "Risk in Contemporary Society," *Connecticut Insurance Law Journal* 6 (2000).
17. Ibid, 395.
18. Y Miaoui and N Boudriga, "Enterprise security economics: A self-defense versus cyber-insurance dilemma," Wiley 35 (2019).
19. Insurance Act 2015, s.3.
20. Ibid, s.3(4).
21. Ibid, s.3(5)(d).

NOTES

22. "Cybersecurity Pros Name Their Price as Hacker Attacks Swell," Bloomberg, 2019, accessed 31st October 2021, https://www.bloomberg.com/news/articles/2019-08-07/cybersecurity-pros-name-their-price-as-hacker-attacks-multiply.
23. Ibid.
24. Marine Insurance Act 1906, s.33(1).
25. Insurance Act 2015, s.10.
26. Ibid, s.11.
27. *Democratic Governance Challenges of Cyber Security*, (DCAF Horizon, 2015).
28. ibid.
29. M Weber. *The Profession and Vocation of Politics. In Political Writings* (Cambridge: Cambridge University Press 2000). 309-369.
30. As explored in Martin. *Short Cyber weapons are called viruses for a reason: statecraft, security and safety in the digital age.*
31. D Woods and R Bohme, "How Cyber Insurance Shapes Incident Response: A Mixed Methods Study," *The 20th Workshop on the Economics of Information Securit* (2021), https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-woods.pdf.
32. [2005] Lloyd's Rep I.R 544, para 19.
33. Ibid.
34. As this type of clause falls outside of the scope of s.11 of the Insurance Act 2015 this would not be a hindrance for the insurer who wants to be relieved from the liability for the assured's breach of this term.
35. How insurance would define offensive cyber operations for this purpose is worth further exploring in future academic writing. Similarly, clear rules would need to be established setting out when the reinsurance could be relied upon by insurers.