Gimme Shelter: A Proposed Civil Liability Framework for Disrupting Botnets, with a particular focus on Smart Devices

Iain Nash[1]

1.1 Introduction

It is a well-known paradigm that when a specialist is presented with a problem that falls within their area of expertise, their response to the problem will be built around the tools of their trade. In response to this effect, Maslow (1966) coined the phrase 'if the only tool you have is a hammer, [you] treat everything as if it were a nail'.[2] When it comes to complex, multi-faceted challenges which intersect with law, technology and cybersecurity standards, this phrase is especially apt. It outlines very effectively one of the prime reasons why it is difficult for an effective, sustainable and scalable solution for the disruption of Botnets to be developed because, not only must such a proposal be understood and accepted by all of the distinct entities involved as the most effective solution, it must also align with their individual incentives. Therefore, the challenge is not only technical in nature, but is also economic and political. When coordination between experts fails, proposals can frequently result in the development of 'local' solutions, built from hammers wielded by distinct specialists, as opposed to a global solution which is built using coordinated and interlocking tools from the underlying disciplines.

This paper proposes a novel legal methodology aimed at disrupting Botnets, using civil as opposed to criminal law. Although there have been successful Botnet take downs in the past,[3] and these take downs have been completed by the coordinated action of various entities in multiple countries,[4] a sustainable and persistent economic solution to deal with Botnets does not yet exist. This proposal is based on the framework outlined in Nash (2020),[5] and although the methodology will work with all forms of Botnets, the focus outlined in this paper will be on Botnets whose endpoints are compromised mostly of Smart Devices.[6] The choice of Smart Devices as a focus for this paper was made as a subset of these devices, colloquially known as the 'Internet of Things' (IoT) which can be considered as ordinary devices which have been augmented by the addition of a CPU and an internet connection, have been a particular effective target for Botnet operators. This effectiveness is partly due to the fact that such devices, unlike a laptop, phone or tablet, are normally activated on a permanent basis which provides good 'uptime' for the Botnet operator and are not accessed by their owners or operators on a regular basis and as such their 'at rest' behaviour can be considered as mostly invisible to their owners or operators. Furthermore, there have been a number of well documented examples of this type of device having particular weak security parameters which allow for an easier compromise when compared to other forms of software.[7]

---

1 School of Law, Queen's University Belfast. Email: inash01@qub.ac.uk. The author thanks the contributions and support from Prof. Daithi MacSithigh and Dr. Philip O'Kane.

2 Abraham H Maslow, *The Psychology of Science* (1st edn, Harper Collins 1966) 15.

3 See, for example Daan de Graaf, Ahmed F Shosha and Pavel Gladyshev, 'BREDOLAB: Shopping in the Cybercrime Underworld' in Marcus Rogers and Kathryn C Seigfried-Spellar (eds), *Digital Forensics and Cyber Crime*, vol 114 (Springer Berlin Heidelberg 2013) <http://link.springer.com/10.1007/978-3-642-39891-9_19> accessed 22 August 2020.

4 An excellent example of such cooperation is outlined in Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (1st edn, Doubleday 2019).

5 See, for example Iain Nash, 'Cybersecurity in a Post Data Environment: Considerations on the Regulation of Code and the Role of Producer and Consumer Liability in Smart Devices' [2020] Unpublished Working Paper <https://iainnash.ie/content/Cybersecurity_In_A_Post_Data_Environment.pdf>.

6 A Smart Device is defined as a device which has both a CPU and an internet connection.

IoT devices were also chosen as the focus for this paper as they can be considered as a 'gateway' to the physical world from cyberspace. This gateway means that a Botnet can carry out an act which can have direct physical consequences as opposed to 'merely' virtual ones, and as such, Botnets which utilise Smart Devices can be a threat to our personal safety as well as to our online security. This physical security risk, which is quite a recent development, further underlines why a rigorous yet applicable framework for tackling Botnets is required as when it comes to IoT, cybersecurity is synonymous with personal safety, as we can now have IoT devices in our homes, our cars and even, in ourselves.[8]

1.2 The Challenges posed by Botnets

Botnets are tools which are used by criminals to conduct cybercrimes and consist of a network of compromised devices (hereafter referred to as nodes) which will run specific commands in coordination with other nodes within the Botnet and under the command of the controller of the Botnet. The word Botnet is a portmanteau of 'Robot' and 'Network',[9] and the term succinctly captures the distributed ability for the operator of the Botnet to have their will imposed on both the devices under their control, and the third party devices which are being targeted in the attack.

The threats posed by Botnets have evolved over time and have altered as our relationship and dependence on remote services has increased. The first generation of Botnets was primarily associated with the sending of spam messages, an activity which continues to this day. Stewart (2008) summarises the activities of the largest Botnets who were involved with the sending of spam from the early 2000s until 2008 where it was believed that the top ten Botnets were able to send c. 135 billion messages per day on a collective basis.[10] This equates to c. 20 messages sent to every person in the world, per day with the majority of these Botnets focused on sending messages related to the sale of pharmaceutical products. Krebs (2012) notes that in 2012, the cost to companies in terms of both indirect costs associated with spam messages (such as lost productivity) as well as direct costs such as the cost of email security programs was c. $140 billion,[11] yet the revenues associated with these activities were in the low hundreds of millions of dollars per year. Therefore, the externalities associated with the sending of spam were many orders of magnitude higher than their underlying worth. More modern Botnets appear to have moved away from sending spam as their primary activities, most likely due to the prospective returns from more lucrative activities such as ransomware and bank theft, which is outlined in more detail further on in this paper.

Distributed Denial of Service (DDoS) attacks were the main activity associated with the next generation of Botnets, although the activities also continue to this day. DDoS attacks occur when an online resource (such as a website) is flooded with requests, so that the number of requests being made per second exceed the capacity of the resource, and thus render it unavailable to legitimate users. DDoS attacks can be used to deny access to government services, commercial entities and information sources such as news sites. Botnets are an excellent vehicle to conduct DDoS from as the technical requirements to conduct the attack is very simple, so much so that any device that has an internet connection will suffice, the

7 See, for example Dilara Acarali and others, 'Modelling the Spread of Botnet Malware in IoT-Based Wireless Sensor Networks' (2019) 2019 SECURITY AND COMMUNICATION NETWORKS 1; and Huichen Lin and Neil W Bergmann, 'IoT Privacy and Security Challenges for Smart Home Environments' (2016) 7 Information 44.

8 See, for example, Muireann Quigley and Semande Ayihongbe, 'Everyday Cyborgs: On Integrated Persons and Integrated Goods' (2018) 26 Medical Law Review 276.

9 Jennifer A Chandler, 'Liability for Botnet Attacks' (2006) 5 Canadian Journal of Law and Technology.

10 Joe Stewart, 'Top Spam Botnets Exposed' *Secureworks* (7 April 2008) <https://www.secureworks.com/research/topbotnets> accessed 13 September 2020.

11 Bryan Krebs, 'Who Is behind the World's Largest Spam Botnet?' [2012] Krebs on Security <https://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/> accessed 13 September 2020.

immense number of nodes in a large Botnet, which are often from a mix of geographies, will be able to deliver, as reported by Singh and Sharma (2019) access requests in excess of 5 gigabytes per second.[12] The authors also note how the growth of Botnet bandwidth capability has been reported at 9% per quarter and that this growth rate is stable, reflecting a doubling of capacity every 24 months.[13]

The latest (at the time of publication) generation of Botnets have developed new attack techniques which are substantially more lucrative than previous methodologies. These are focused on banking related theft and ransomware[14]. Banking theft Botnets, such as *Zeus* or *GameOverZeus* are focused on targeting devices which are used to access a person's bank details and the malware will look to harvest the person's banking credentials in order to effect unauthorised transfers. Ransomware is a different methodology, which is where the effected device has its disks encrypted by the Botnet operator, who will only decrypt the device once a ransom has been paid. These activities can be many orders of magnitudes more lucrative to the Botnet operator when compared to 'traditional' Botnet activities. This is because the owner of each compromised node is now a potential victim as well as providing the infrastructure to expand the Botnet.

1.3 The economics behind Botnets

The underlying economics behind Botnets are complex, as there are multiple types of Botnet operators who have differing motivations and incentives. Botazzi and Me (2014) offer a comprehensive overview of the revenue models associated with Botnets,[15] and note how, just as has happened in the legitimate economy, there are now cybercrime 'outsourcing partners' who can provide ready-made Botnets to nefarious individuals who have a wish to conduct cybercriminal activities and have the resources to 'lease' the required infrastructure but who lack the technical skills to develop the Botnets themselves. Indeed, the authors note how there is quite a sophisticated supply-chain infrastructure which includes technical and customer support for these cybercriminal customers. The authors' work predates the growth in Ransomware as economic activity but covers most other standard Botnet activities.

DDoS is a prevalent and persistent form of Botnet attack yet it is not an particularly lucrative endeavour. The Mirai Botnet, which was comprised of mostly IoT devices due to the weak security associated with the class of device as a whole,[16] was the largest and most powerful Botnet to-date (2017) and was able to generate enough false requests to temporarily bring down servers which were part of the backbone of the internet. However, these activities themselves are not necessarily lucrative as IoT devices will, when compared to other Smart Devices, tablets or computers will not contain valuable personal information such as banking or payment details, and unless the activity has been commissioned by a cybercriminal sponsor, won't generate income as a percentage of requests served. Indeed, Schwartz (2017) notes how the operator behind the Mirai Botnet sought to blackmail the providers of large financial services such Barclays and Lloyds Banks with the threat of being able to deny their customer the ability to access their accounts online, making the enterprise somewhat akin to a rudimentary form of ransomware.[17]

---

12 Rajeev Singh and TP Sharma, 'Present Status of Distributed Denial of Service (DDoS) Attacks in Internet World' (2019) 4 International Journal of Mathematical, Engineering and Management Sciences 1008.

13 ibid 1011.

14 It is important to note that phishing emails, which can be sent from Botnets, are an important part of the ransomware process.

15 Giovanni Bottazzi and Gianluigi Me, 'The Botnet Revenue Model', *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14* (ACM Press 2014) <http://dl.acm.org/citation.cfm?doid=2659651.2659673> accessed 22 September 2020.

16 Constantinos Kolias and others, 'DDoS in the IoT: Mirai and Other Botnets' (2017) 50 Computer 80.

DDoS however, is an extremely effective tool when it comes to supporting the actions of a private individual, group or Nation State who wishes to cause disruption as an end goal. Aslanoglu and Tekir (2012) note how Botnets were used in Estonia in 2007 and in South Georgia in 2008 as part of a quasi-political cyberoperation and also to 'punish' the recipients for taking part in actions against Russia.[18] These attacks demonstrate how DDoS attacks, although they may not result in direct revenue for the Botnet operators, can support other forms of cybercrimes. Kolias et al (2017) note how they have observed a derivative of the Mirai Botnet which was able to initially compromise IoT webcams, but from there was able to infect the routers in the network, which outlines how IoT devices can be exploited as the 'weak links' in a network's cybersecurity,[19] and how a Botnet variant which would be associated with DDoS can also be used as part of a more intricate cybercriminal strategy.

Ransomware was one of the first economically lucrative forms of Botnet activities, and has come to the fore of public attention following the *WannaCry* and *NotPeya* attacks,[20] although ransomware activities can be traced back as far as the 1980s.[21] Krebs (2017) notes how the *GrandCrab* ransomware has been able to generate revenue in excess of two billion dollars,[22] although work by Pacquet-Clausen et al. (2019) suggest that actual payments made following a ransomware attack may be over-hyped.[23] In the context of Botnets, ransomware is a type of payload that is delivered to a node in a Botnet at the behest of the Botnet operator and makes the device inoperable until a ransom has been paid. From a technical perspective, the device is encrypted and the key will only be provided once payment has been received. The *WannaCry* and *NotPetya* examples focused on non IoT and Smart devices, and it is a somewhat common belief that Smart Devices aren't a target for Ransomware as they don't hold valuable personal data, can easily be reset and their 'denial of service' won't result in a large imposition for their owners. This may be somewhat true for personal users' IoT devices, but IoT and Smart Devices have now become common in industry and have become integral in Healthcare,[24] the Maritime Industry,[25] and in Industry 4.0,[26] as well as in providing data for the administration of cities and towns (traffic cameras, air pollution).[27] Furthermore, given the already discussed weak inherent security settings which is often present in IoT devices, they can be considered as a means to effect entry into a system as opposed to being the ultimate goal.[28]

17 Matt Schwartz, 'Mirai Malware Attacker Extradited from Germany to the UK' *Bank Info Security* (31 August 2017) <https://www.bankinfosecurity.com/mirai-malware-mastermind-extradited-from-germany-to-uk-a-10247> accessed 22 September 2020.

18 Rabia Aslanoglu and Selma Tekir, 'Recent Cyberwar Spectrum and Its Analysis' (2012).

19 Kolias and others (n 13).

20 It must be noted that *Wannacry* is a worm as opposed to a Botnet. It is included in this paper due to the publicity it generated surrounding ransomware.

21 Azka Wani and S Revathi, 'Ransomware Protection in IoT Using Software Defined Networking' (2020) 10 International Journal of Electrical and Computer Engineering (IJECE) 3166, 3167.

22 Brian Krebs, 'Who's Behind the GandCrab Ransomware?' (*Krebs on Security*, 2019) <https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/> accessed 23 March 2020.

23 Masarah Paquet-Clouston, Bernhard Haslhofer and Benoît Dupont, 'Ransomware Payments in the Bitcoin Ecosystem' (2019) 5 Journal of Cybersecurity tyz003.

24 AK Sarangi and others, 'Healthcare 4.0: A Voyage of Fog Computing with IoT, Cloud Computing, Big Data and Machine Learning' in S Tanwar (ed), *Fog Computing for Healthcare 4.0 Environments* (Springer 2021).

25 M Plaza-Hernandez and others, 'Integration of IoT Technologies in the Maritime Industry', *Advances in Intelligent Systems and Computing* (Springer 2021).

26 M Swarmi, D Verma and VP Vishwakarma, 'Blockchain and Industrial Internet of Things: Applications for Industry 4.0' in P Bansal and others (eds), *Proceedings of International Conference on Artificial Intelligence and Applications.* (Springer 2021).

27 See, for example, Andrea Zanella and others, 'Internet of Things for Smart Cities' (2014) 1 IEE Internet of Things Journal 22.

28 See, for example, Acarali and others (n 7).

Accordingly, IoT is becoming a more interesting and lucrative target for ransomware as the locking up of the IoT devices will cause a failure in industrial processes as the lack of data being produced by the IoT devices will prevent systems from operating. Therefore, we may soon reach the stage where complex systems can be halted due to their dependence on IoT devices, and so a ransomware attack becomes an attack on a process as opposed to a more data-based attack.

Putman et al (2018) note how banking related Botnets such as Zeus and its derivatives, which are based on accessing personal financial information,[29] and making unauthorised transfers of funds from their victim's accounts. These Botnets are normally targeting devices which are actively used by their victims (such as laptops, tablets and Smart phones) as the Botnet operator is looking for the victim's financial account credentials, which are unlikely to be found on an IoT device. Sarojini and Asha (2019) note how the attack vectors for these type of Botnets are normally based around 'drive by' downloads and other surfaces which have constant user interaction.[30] Although this niche isn't one which is associated with IoT and other such Smart Devices, the proposal outlined in this paper will still be applicable in preventing these types of attacks.

Click Fraud is another form of, relatively recent, Botnet activity. Click Fraud is where a Botnet will be instructed to click ads on a website, which are presented on a 'cost-per-click' basis with either the intention of depleting the advertising budget of a company, or increasing the ranking of a website, which will increase the bids per click associated with that site.[31] Choi and Lim (2020) estimate that c. 30% of advertising revenue is a result of fraudulent clicks.[32] Similar to DDoS attacks, Botnet operators are normally paid to carry out this activity, as opposed to benefiting directly from the fraud.

1.4 Botnet Legal Challenges

The legal challenges which arise when tackling Botnets are both numerous and technical, as the distributed nature of the a Botnet means that it will invariably span multiple jurisdictions and both law enforcement agencies and legal theorists face the rare circumstance where both the owner of each node of the network is both a victim and perpetrator. This duality has been outlined in detail in van der Wagen and Peters (2020),[33] and the authors note how modern legal systems are based around the principle of having clearly defined perpetrator and victim identities, and when a single actor is both victim (their device has been hacked) and perpetrator (their device has been used in the commission of a crime), the single actor takes on both identities simultaneously and legal operations become complicated with the resulting outcomes normally being suboptimal.

Botnets also have quite a unique and distinct feature in that the damage caused by (and to) each individual node is often very small, while the effect of the network as a whole is substantial. This means that from a law enforcement perspective, the Botnet is treated as a singular device under the direct control of the Botnet operator, as opposed to treating each

29 CGJ Putman, S Abhista and LJM Nieuwenhuis, 'Business Model of a Botnet', *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)* (IEEE 2018) <https://ieeexplore.ieee.org/document/8374500/> accessed 21 September 2020.

30 S Sarojini and S Asha, 'Botnet Detection on the Analysis of Zeus Panda Financial Botnet' (2019) 8 International Journal of Engineering and Advanced Technology 1972.

31 Shahrear Iqbal and others, 'FCFraud: Fighting Click-Fraud from the User Side', *17th International Symposium on High Assurance Systems Engineering* (IEEE Computer Society 2016).

32 Jin-A Choi and Kiho Lim, 'Identifying Machine Learning Techniques for Classification of Target Advertising' (2020) 6 ICT Express 175.

33 Wytske van der Wagen and Wolter Pieters, 'The Hybrid Victim: Re-Conceptualising High-Tech Cyber Victimization through Actor-Network Theory' (2020) 17 European Journal of Criminology 480.

node distinctly. This makes sense, as it means that law enforcement resources are focused on a singular task, and that the consequence of the legal action is not limited to the almost infinitesimal value of an individual node. However, this focus on the Botnet as a single entity has potentially limited the scope of legal remedies, as is discussed further on in this paper in more detail.

Furthermore, the challenges presented by Botnets do not even end following the successful take down of a Botnet and the prosecution of its operator. The term 'take down', when relating to a Botnet usually refers to the sink-holing of the network, where the Botnet operator is not longer able to send commands to the network, and the subsequent deletion of the command and control infrastructure. However, most law enforcement agencies do not have the right to purge compromised nodes of malware which will allow the device to pulled into another Botnet, thus we can see how legal action against the operator of the Botnet does not translate automatically into protection for those whose machines had been compromised.

Victims of Botnet attacks will also find their legal remedies stymied. It is normally not possible for the owner of a compromised device to seek damages from the manufacturer of the device, and the third-party victim who suffered, for example, a DDoS will find that the nature of the damage caused will be of a type that is not recoverable in the courts.[34]

Botnets, from a cybersecurity perspective, are also quite problematic, as there is a legal challenge as the conduct which is carried out by cybersecurity researchers is frequently equivalent, from a legal perspective, to that of the operators of Botnets. This can limit research into Botnets and can actually result in the supporting of Botnet operators as their *modus operandi* may not make it into the cybersecurity research community in a timely manner. Gerard (2020) outlines how researchers who were able to take over the TORPIG Botnet suddenly found themselves receiving data such as bank account details, credit card numbers and other personally identifiable information,[35] and their actions can be seen as violating cybercrime statutes in their jurisdiction. Gerard notes similar examples, where the actions of cybersecurity researchers differ only from the actions of the cybercriminals in the matter of their intent. It is possible for the cybersecurity researcher to perform modifications to the underlying malware so that it may no longer propagate as was done by Pacquet-Clouston et al. (2018),[36] but the distributed nature of communication within the network means that the researcher may still come to possess personal data or will still be integral to a cyberattack on a third party. Vihul et al (2012) also notes how there are very few examples of specific pieces of legislation which make provision for cybersecurity research.[37]

Therefore, we can see how, apart from some specific exceptions,[38] cybercrime legislation has failed to take into account the nature of how cybersecurity research works in practice and places legal hurdles in the path of individuals and institutions who are attempting to disrupt them, thus place prohibition on research into the very activities which the legislation is outlawing. Furthermore, it is not proposed that the solution to this issue is the registration or regularisation of cybersecurity researchers which would not be feasible given the already discussed distributed and informal network of researchers.

34 The specific challenges to legal action are outlined in Nash (n 5).

35 Grant Gerard, 'Botnet Mitigation and International Law' (2020) 58 Columbia Journal of Transnational Law 191, 203–205.

36 Masarah Paquet-Clouston, David Decary-Hetu and Olivier Bilodeau, 'Cybercrime Is Whose Responsibility? A Case Study of an Online Behaviour System in Crime' (2018) 19 Global Crime 1.

37 Liis Vihul and others, 'Legal Implications of Countering Botnets' (NATO Cooperative Cyber Defence Centre of Excellence 2012).

38 See, for example, the Good Faith exemptions which are exceptions to prohibited actions in the Digital Millennium Copyright Act, Public Law 105-304

2.1 The Current State of Botnet Disruption

When an entity is looking to disrupt a Botnet using a legal methodology, there are a number of options open to them which depend on whether they are a Nation State, a Law Enforcement Body or an individual.

From a Nation State perspective, there is an obligation under the norms of Public International Law, as outlined in the *Corfu Channel* case,[39] for a Nation State to prevent actions carried out directly by State entities, as well as activities carried out by non-state entities of which the State was aware which are contrary to the international legal rights of other States. *Corfu* involved two British ships which had struck mines in Albanian waters. The ships were traversing an international strait and it was held that while it was not proven that the Albanian government itself was responsible for the placing of the mines, the Court believed that the Government was, at the very least, aware of the danger, and as such should have warned ships using the strait of the danger.

Buchan (2016) outlines the elements which must be present for such an obligation to be established;[40] the actions must be attributable to the State and it must be found that the State had 'effective control' over the non-state actor, alternatively it is be possible to demonstrate that responsibility should attach to the State if it has failed to take a positive action against the non-state actor where it had a primary obligation to do so. Buchan notes how when these principles are applied to cyberactivities, the issue of attribution can be difficult due to the ability of the perpetrators to mask their locations. This is particularly appropriate to Botnets, where the Botnet controller is not required to be within the same jurisdiction(s) of the nodes which carry out the cybercrime activities. Buchan suggests that one method of solving this issue is the creation of an international treaty which will create an enforceable obligation on Nation States, within whose borders cybercriminals operate to the detriment and harm of citizens in other Nation States.

Couzigou (2018) examines the recent cyberattacks which were conducted against Estonia by what was believed to be Russia, and the Stuxnet worm which was deployed against Iran by what is thought to have been a joint enterprise between the United States of America and Israel,[41] and finds that Public International Law is not a viable avenue for hindering such cyberattacks because of the aforementioned attribution problems. Couzigou's findings are supported by work of Zetter (2014),[42] and Egloff (2019),[43] who affirm the practical difficulties in correctly establishing attribution beyond mere supposition. Couzigou also suggests the development of a treaty, echoing the suggestion by Buchan, but given the slow speed at which the Council of Europe's Treaty on cybercrime has been adopted, and the current state of geo-political tensions, there is little to suggest that there is an appetite for such a Treaty and there is nothing to suggest that it would be ratified by the countries which engage covertly in cyberoffensive operations.

Application of Public International Law is not the only avenue which is open to entities involved in the fight against Botnets. A, theoretically at least, simpler approach would be the

39 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* [1949] Rep 1 (ICJ).

40 Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 Journal of Conflict and Security Law 429.

41 Irène Couzigou, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations' (2018) 32 International Review of Law, Computers & Technology 37.

42 Kim Zetter, *Countdown to Zero Day* (1st edn, Broadway Books 2014).

43 Florian J Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia' (2019) 41 Contemporary Security Policy 1.

an application of ordinary criminal law, and where the Botnet operations are international in nature, such an application can be supported by mutual assistance treaties enacted between countries. This approach has proven to be a valid means to prosecute the operators of Botnets and limit their scope for conducting cybercrimes, and will normally involve cooperation between law enforcement bodies in differing jurisdictions, as well as cooperation between key online infrastructure providers and law enforcement to both directly limit the potential spread of a Botnet and also to gather evidence. Examples of this approach are outlined in detail by Nadji (2013),[44] and in their updated work Nadji et. al. (2015),[45] where they note the coordination challenges faced in taking down the Conficker Worm, the Mariposa Botnet and a number of other malicious and promiscuous examples of malware.

In the Conficker example, the Botnet controller was able to communicate with the nodes in the Botnet by means of an algorithm which would look for a finite and determinable set of domain names, which were known to the nodes. To combat the worm, a working group was formed who coordinated with domain registrars to sink-hole the traffic and to be able to operate sufficiently quickly so that the possible range of domains (as determined by the reverse-engineering of the underlying malware) were pre-registered by the Working Group, enabling them to deny the controller access.[46] However, this coordinated model required cooperation from domain registrars and registries as well as the support from Top Level domain registrars in hundreds of countries. Such support was only possible because the extent of the infection caused by the worm, as it has spread to an estimated 15 million devices globally.[47] While this approach was mostly effective in stopping the worm from spreading, it was not until a patch had been developed and released by Microsoft was the risk reduced. It should also be noted that the developer of Conficker has never been identified and therefore, no prosecution has been able to take place, and there are still conficker infections taking place (albeit at an almost infinitesimal rate when compared to its peak) as not all devices have been patched, despite the patch being available for many years.

A similar approach was taken with the Mariposa Botnet which was heavily concentrated in Spain, where again the domains were taken under the control of the working group formed to counter the Botnet. However, in this case, the Botnet operator was able to bribe an employee in one of the domain registrars to return access to some domains, which enabled him to resurrect the Botnet, and so the working group operations had to restart. The work carried about by the working group enabled evidence to be presented to Spanish Law Enforcement agencies who were able to arrest people suspected of being involved in the operation of the Botnet, and cross-border cooperation ensured that further people were arrested in Slovenia and the USA.[48] Nadji et al (2013) also relate the example of how cooperation between Law Enforcement bodies and technical groups resulted in the seizing of the servers which ran the DNSChanger malware as well as the takedown of hosting networks, who provided 'bulletproof' hosting to people with no Terms of Service, which hosted Botnets and other cybercriminal related applications.

---

44 Yacin Nadji and others, 'Beheading Hydras: Performing Effective Botnet Takedowns', *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications* (Association for Computing Machinery 2013).

45 Yacin Nadji, Roberto Perdisci and Manos Antonakakis, 'Still Beheading Hydras: Botnet Takedowns Then and Now' (2015) 14 IEEE Transactions on Dependable and Secure Computing 535.

46 Sink-holing is a technique where machines which try to access a given domain name are directed away from the intended server and instead are brought to a server under the control of the registrar.

47 Patrick Howell O'Neill, 'Conficker Worm Still Spreading despite Being Nearly 10 Years Fold' *Cyberscoop* (8 December 2017) <https://www.cyberscoop.com/conficker-trend-micro-2017/> accessed 10 September 2020.

48 Bryan Krebs, 'Mariposa' Botnet Authors May Avoid Jail Time' *Krebs on Security* (4 March 2010) <https://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/> accessed 9 September 2020.

Therefore, we can see that when there is a threat on a 'global' scale, the coordination that has been outlined in various stages which exists between cybersecurity stakeholders on both a formal and informal basis can be leveraged to provide information to the Law Enforcement which can be used to initiate criminal proceedings. However, given that Botnets are normally an international enterprise, in order for criminal proceedings to be successful, where are there multi-jurisdictional elements there must be:

- A specific prohibition against the actions taken by the Botnet operator in all concerned jurisdictions, or a recognition that the crime is substantive in the requesting Member State[49]; and
- An agreement between the two countries which allows for extradition of the Botnet operator (if extradition has been sought); and
- The political will for the crime to be investigated and the perpetrators to be stopped in all jurisdictions.

Therefore, it is clear that if the Botnet is operating in a jurisdiction which is either providing clandestine instructions or support, or which is turning a blind-eye to its operations, it will not be possible to engage in ordinary multilateral criminal proceedings as a means to shutdown the Botnet.

Furthermore, neither the sink-holing of domains nor the prosecution of the Botnet operator will necessarily result in the underlying malware being removed from a node and as such, the threat of that device being recruited into a Botnet is not removed. Krebs (2010) notes how the FBI believe that the Mariposa Botnet has been resurrected by a new Botnet operator, even though its original operator was arrested.[50] Accordingly, the application of the criminal law can be considered as a valid option for the hindering of large-scale, international Botnets but even if successful, it will not necessarily stop the operation of the Botnet over the medium term, and it is not an option when the Botnet operator is conduction operation with either implicit or explicit support from the Nation State where the operators reside.

Finally, below the level of the application of the criminal law, there is the action of individual citizens who operate independently of the entities associated with a Nation State. The theory that private citizens are responsible for policing the actions of others has been summarised by e Silva (2018) who notes how 'cyber vigilantes' are individuals (or groups of individuals) who act in a retaliatory manner to cybercriminal acts.[51] The author notes how, in response to the threat posed by *Mirai*, a Botnet which spread through IoT devices, a cyber vigilante created *BrickerBot* which was developed to seek out IoT devices which were vulnerable to Mirai and to corrupt their storage ability so as to incapacitate them permanently.[52] This action, however, is a cybercrime itself, and equivalent to Mirai. A more positive example of 'vigilantism' was outlined by Khomani and Solon (2017) who detail how an individual was able to halt the spread of the *Wannacry* ransomware through the purchase of a domain which acted as a kill-switch for the software.[53] This individual, later identified as Marcus Hutchins,[54] had conducted the sink-holing act accidentally, as having read the source code of the worm, he was looking to

49 See, for example, Art 2(2) of the European Council Framework Decision 2002/584/JHA which will enable extradition to be granted even if the underlying act is not a criminal act within the Member State, so long as the act is punishable with at least three years of imprisonment in the requesting Nation State.

50 Krebs (n 39).

51 Karine K e Silva, 'Vigilantism and Cooperative Criminal Justice: Is There a Place for Cybersecurity Vigilantes in Cybercrime Fighting?' (2018) 32 International Review of Law, Computers & Technology 21.

52 ibid 26.

53 Nadia Khomani and Olivia Solon, '"Accidental Hero" Halts Ransomware Attacks and Warns: This Is Not Over' *The Guardian* (London, 13 May 2017) <https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack> accessed 30 August 2020.

examine its communications in more detail.[55] However, underlying intention aside, it demonstrates how cyber vigilantism can be of benefit in the fight against Botnets.

The examples highlight the challenges associated with vigilantism, or actions conducted by private individuals which are independent of official agencies. In the *Brickerbot* example, such activity is really no different from that of the act which it is responding to and from a holistic perspective, cannot be seen as improving the security or safety of others. While the *WannaCry* example is more positive, it is the exception rather than the rule as without such an easily implemented kill-switch, which was a unique artefact of this particular codebase, vigilante interventions are not normally so simple or as effective in stopping the spread of malware.

A modified form of the cyber vigilante theory has been outlined by Miraglia and Casenove (2016), who propose that cybersecurity professionals should have access to the same 'arsenal' as the Botnet operator.[56] This 'active defence' suggestion is based around the principle that devices which have become nodes in a Botnet should be (forcefully) given an 'antidote' which will remove or nullify the malware. This suggestion does have the benefit of actively removing the number of the nodes which are available to the Botnet operator, but it does so as the expense of device security and, as mentioned earlier in this document, reduces the cybersecurity professional or researcher to effectively the same role as the Botnet operator from a legal perspective. It also fails to address the root cause of the issue which is the failure of the developer to deploy or make a patch available, or the failure of the device operator to apply the patch.

What is of much more interest, and comprises a key part of the proposed framework is the fact that there appears to be a relatively sophisticated if unchaperoned communications network between cybersecurity researchers, practitioners and relevant nation state agencies. This can be seen in the work by Greenberg (2020) who notes that when Hutchins was inadvertently carrying out his sink-holing operations he was in contact with other cybersecurity researchers and practitioners, some of whom were directly effected by the ransomware and providing and receiving information about the worm.[57] This behaviour has been demonstrated as being present during other threats, such as that outlined by Zetter (2014) when cybersecurity companies were engaging with one another and with ISPs when the effects of Stuxnet were starting to be felt,[58] by Greenberg (2019) who reports a similar cooperation and exchange of information arising from the consequences of *NotPetya.*[59] De Graaf, Shosha and Gladyshev (2013) outline in great detail the level of cooperation between private companies associated with cybersecurity and law enforcement agencies in the take down of a Botnet,[60] and such activities have been repeated by companies such as Microsoft, who work with other software companies and law enforcement to taken down Botnets.[61]

---

54 Karine incorrectly attributes the sink-holing of the Wannacry ransomware to Darien Huss, a cybersecurity researcher, whereas the action was performed by Marcus Hutchins. Huss did speak with Hutchins during his sink-holing operation but was not the purchaser of the domain. Hutchins was subsequently arrested and convicted in the United States for having previously developed a hacking tool called Kronos. Full details of both the stop of *Wannacry* and his arrest have been written by Andy Greenberg, 'The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet' *Wired Magazine* (12 May 2020) <https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/> accessed 30 August 2020.

55 Khomani and Solon (n 44).

56 Armando Miraglia and Matteo Casenove, 'Fight Fire with Fire: The Ultimate Active Defence' (2016) 24 Information and Computer Security 288.

57 Greenberg (n 45).

58 Zetter (n 33).

59 Greenberg (n 4).

60 de Graaf, Shosha and Gladyshev (n 3).

61 David E Sanger, 'A Botnet Is Taken Down in an Operation by Microsoft, Not the Government' *The New York Times* (New York, 10 March 2020) <https://www.nytimes.com/2020/03/10/us/politics/microsoft-botnets-malware.html>

The actions taken by Microsoft (and others) are of particular interest. Two recent take-downs are of note; the Necurs Botnet and the TrickBot Botnet. The Necurs Botnet takedown arose following Microsoft alleging that they have suffered harm as a result of the actions of the Botnet operator,[62] due to the damage caused to their reputation. However, their approach in the TrickBot approach was based on trademark violations,[63] which was a new approach taken by the Digital Crimes Unit,[64] and potentially simpler to justify than the earlier attempts which required a veritable smorgasbord of alleged infringements. This is because the Tickbot allegations of trademark violations was based on the defendants using Windows SDKs to develop the Botnet. In both actions, the reports by Microsoft outline the time and effort which goes into identifying the key parameters of the Botnets operations,[65] but even at the end of their civil actions, there are no remedial actions enacted against the nodes of the Botnet, which means that it is possible for the Botnet to be 'rebuilt' by a new Botmaster and, as was demonstrated by TrickBot, the enforcement actions will only work for server operators who will respect and act on a United States court order.

As has been outlined earlier in this document, in order for a Botnet mitigation model to be effective, it must fit within the parameters of how each entity involved operates, and in order for the effects be long lasting, it must remove the underlying malware from the compromised system. Therefore, given that there appears to be a strong and persistent information flow between cybersecurity practitioners, professional and agencies which have been observed over the past decade and a half, then such interaction should be built into the proposed solution framework, as opposed to applying methods which try to alter it or fail to take it into account, and any proposed approach must also tackle the underlying malware.

3.1 The Threats posed by Botnets in the Future

To date, the work outlined in this paper has been retrospective in nature and has been developed through the lens of Botnets past. It is important to note how, at the time of publication, it is probable that consumers are approaching an inflection point with regard to Smart Devices and also with regard to the nature of threats posed by Botnets. Schneier (2018) notes that consumers went through an inflection point with the development of what he terms 'Internet+' devices, which was the first combination of 'the internet' and 'things' and 'us',[66] and notes how this became very tangible in 2007 with the advent of the iPhone which was the first mass adopted Smart Device which users interacted with quite differently from a normal computer.[67]

However, it is important to note that this device succeeded because of the widespread availability of consumers to access the internet 'on-the-go'. The advent of '3G' and '4G'

accessed 30 August 2020.

62 *Microsoft Corporation v John Does 1-2, Controlling Computer Botnets and Thereby Injuring Plaintiff and their Customers* [2020] United States District Court for the Eastern District of New York 1:20-cv-01217-LDH-RER.

63 *Microsoft Corporation v John Does 1-2, Controlling a Computer Botnet and thereby Injuring Plaintiffs, and their Customers and Members* [2020] United States District Court for the Eastern District of Virginia 1:20-cv-1171 (AJI/DD).

64 Brian Krebs, 'Microsoft Uses Trademark Law to Disrupt Trickbot Botnet' *Krebs on Security* (12 October 2020) <https://krebsonsecurity.com/2020/10/microsoft-uses-copyright-law-to-disrupt-trickbot-botnet/> accessed 13 October 2020.

65 See, for example Tom Burt, 'New Action to Disrupt World's Largest Online Criminal Network' (10 March 2020) <https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/> accessed 13 October 2020; and Tom Burt, 'New Action to Combat Ransomware Ahead of U.S. Elections' (*Microsoft Blog*, 12 October 2020) <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/> accessed 13 October 2020.

66 Bruce Schneier, *Click Here to Kill Everybody* (WW Norton & Company 2018) 8.

67 ibid 3.

communications spectrum allowed Smart Devices to function with remote data at sufficient speeds to provide consumers with the ability to check emails and listen to music in 2007 to watch full length HD movies with ten years. 5G, the current next generation of carrier spectrum is measured in gigabits per second (as opposed to megabits per second) and although wireless, can outperform fibre cable. This speed will enable Smart Devices to be in real time communication with other Smart Devices using exchanged data to power programmes and algorithms. Such a scenario will allow, for example, self driving cars to be in constant communication with other cars in order to manage safety as well as engaging with cars and data aggregators further afield to determine route optimality.
This factoring of large amounts of real-time data on a continuous basis introduces new risk factors which Botnets are a particular threat to. It has been reported how Simon Weckert crated a simple Botnet which consisted of 99 mobile phones in a wheelbarrow and used these to spoof traffic data in Google maps,[68] and reduce the traffic flow near his residence. Botnets will be able to either deliver large chunks of spurious or erroneous data to a target, or to deny access to a network resource and thus interrupt Smart Devices which rely on continuous data flow. The Google Maps example was a relatively benign exercise, but a Botnet made of kitchen appliances could feed scheduled usage data into a power grid, or could flood traffic resources with spurious requests. The proposed methodology to disrupt Botnets outlined in this paper has been developed in the context of both past and present Botnet attacks, as well as likely threats arising from technology which is new or in the process of being released.

Accordingly, when evaluating the proposed framework, it is important to view the threat of IoT Botnets not only in context of past behaviour but also in the context of expected IoT behaviour and usage in the short to medium term. The current political debate surrounding security issues related to the roll-out of 5G licences is focused on threat that a supplier of either hardware or software to the network can pose,[69] as opposed to how other threat actors can use Smart Devices and their (expected) reliance on high frequency data which will be enabled by 5G.

4.1 The Proposed New Framework

A literature review of proposed solutions to the Botnet problem identifies an interesting trait emerging in the writings of legal theorists on the matter; Botnets are invariably treated as a singular unit.[70] It is most likely that this occurs due to the fact that, from an information security perspective, targeting the nodes of an Botnet is less efficient than targeting the command and control centre as the Botnet will continue to function with its remaining nodes, and, as discussed already in this paper, from a legal perspective it is more advantageous and effective to operate under the principle that the cybercrime has been committed by the Botnet controller as opposed to the owners of the compromised nodes. Furthermore, the presence of a singular controller behind the Botnet means that the Botnet will work to a either a singular or a series of singular goals which can further encourage the view of a Botnet as a single unit.

---

68 Anmol, ‘A Man Used 99 Phones on a Cart to Create Virtual Traffic Jams on Google Maps’ (3 February 2020) <https://mspoweruser.com/a-google-map-hack-helped-this-man-create-virtual-traffic-jams/> accessed 28 September 2020.

69 See for example Donald Trump, ‘National Strategy to Secure 5G of the United States of America’ <https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf> accessed 27 July 2020; NIS Cooperation Group, ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’ (2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132> accessed 4 October 2020.

70 See, for example, Christopher S. Stewart, ‘Inside the Effort to Kill a Web Fraud 'Botnet'’ and Karine K e Silva, ‘How industry can help us fight against botnets: notes on regulating private-sector intervention’ 2017 31 Int Rev Law Comput Technology 105

Within the legal academic literature, the distributed nature of the Botnet, although usually addressed early in the paper, is not usually discussed again apart from perhaps presenting jurisdictional or additional technical challenges. This trait is interesting, as if we were to propose a simple model of a Botnet's efficacy, it would be directly related to the number of compromised machines within the network and the effectiveness of these machines in achieving the goal of Botnet controller. This can be generalised to the equation below:

$$B=\sum_{i=1}^{N} \rho_i m_i \qquad \rho \in 0,1$$

where B is a Botnet compromising of N compromised individual devices (m) and ρ is a measure of the individual devices' technical capacity to conduct the desired attack. This representation assumes heteroscedasticity among the compromised machines, which is unrealistic given that a compromise of one type of device or operating system will, most likely, lead to the ensnaring of similar devices. Therefore, a more accurate representation of the efficacy of a Botnet is:

$$B_T=\sum_{j=1}^{T} \left(\rho^j \sum_{i=1}^{N^j} m_i^j \right)$$

where it is assumed that the Botnet is comprised of T distinct groups of individual compromised devices,[71] with each group consisting of N devices, each which is assumed to have an identical value for ρ, as they share the same underlying operating system and parameters.[72] Accordingly, when thinking about the Botnet, it is important to recognise that it is not comprised of individual, distinct nodes but rather groups of effectively identical devices.

Furthermore, it is important to recognise that Botnets themselves operate in a competitive environment. As discussed earlier in this paper, Botazzi and Me (2014) outline how there is now a market place for 'Botnet as a Service' type activities where the Botnet is leased to a cybercriminal who wants to carry out a specific action but lacks the skill or time to develop their own Botnet.[73] There are also Botnets which have been created by individuals whose principle goal is the creation of the network itself, however, it is reasonable to assume that these networks, should they reach a scale which allows them to compete with the 'professional' Botnets, will also end up in a criminal marketplace.

Therefore, when it comes to the problem of how to disrupt Botnets, the options aren't restricted to, as frequently presented in the literature, either the removal of the Botnet operator or the cleansing of a device (m) but there is also the third option of targeting the nodes contained within a given group (T), which will have the effect of removing all devices within a given group.

From the perspective of trying to disrupt the Botnet, while technical steps can be taken to reduce the ability of the Botnet to communicate with the Command and Control Server, communicate with other nodes or communicate with the target, the fact that the commands and attacks are usually sent over common protocols,[74] reduces the scope of this defence.

---

71 Note that T refers to groups of compromised machines which have the same operating system and were compromised by the same exploit.

72 There may be some differences in ρ between devices caused by different options and the use by the device, but for illustrative simplicity, these differences can assumed to be zero without changing the result of model.

73 Giovanni Bottazzi and Gianluigi Me, 'The Botnet Revenue Model', *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14* (ACM Press 2014) <http://dl.acm.org/citation.cfm?doid=2659651.2659673> accessed 22 September 2020.

74 A DDOS attack, for example, will consist of ordinary web requests

Technical measures may be taken to attempt to reduce the value of ρ and thus reduce the power of Botnet. However, the specific value of ρ for a given type of machine can be considered as endogenous to the desired outcome and therefore the controller of the Botnet can take steps in the design of their Botnet to maximise ρ while such an option is not open to law enforcement. Finally, reducing the value of ρ, unless it is reduced to zero, or close to zero, will only limit the impact that a given type of compromised machine will have (and indeed, only on a relative rather than absolute basis), it won't reduce the number of compromised machines.

Instead, this paper proposes a hybrid framework, comprised of legal and market driven tools aimed at disrupting Botnets by using the threat of civil liability against the producer or operator compromised nodes to reduce the count of T and m towards zero, which will reduce both the efficacy and the size of the Botnet. It is important to note that for each Botnet there is a critical mass, and that once the size of the Botnet falls below this value it becomes ineffective,[75] and as the Botnet has been driven back towards this value by the inoculation of former nodes, the only way for it to grow again is to find a new type of device to compromise. The objective of the proposed framework is to create an environment where there is constant pressure on effective Botnets to reduce them to below the critical mass and to ensure that any device which has been infected by a Botnet is there for a short, limited time. It is expected that as the count of T is reduced, the Botnet operator will have to accept nodes which have a sub-optimal value of ρ which is an outcome which will also lead to reduced Botnet performance.

Given the homoscedasticity present within the Botnet and also within the wider environment of connected devices, the removal of a type of compromised device will have a multiplicative (as opposed to linear) effect on the reduction of the Botnet and will also limit its ability to regrow. The model aims to inoculate Smart Devices against future ensnarement into a Botnet, solving the problem which is faced by Law Enforcement where removal of the Botnet operator does not permanently remove the nodes from the Botnet.

It should be now clear that this novel approach does not target the Botnet as a singular unit, but instead focuses on the individual devices which make up the Botnet and aims at making it progressively more difficult for the controller of a Botnet to maintain captured devices within the network.

This approach is complimentary towards other coordinate activities which are used to combat Botnets and are outlined earlier in the paper. It is also probable that a successful application of this novel approach will act as a multiplier for existing activities, as the work load for each takedown will now be reduced.

The framework as outlined in Nash (2020) is based on the principles associated with the law of Tort. A tort arises following an action by one party which causes harm or damage to a different party, it is important to note that tortious action does not require a pre-existing relationship between the parties, only the infliction of damage by a party. A tort is not a crime however, it is a civil wrong and as such, there is no requirement for involvement by any law enforcement bodies and there is no requirement for a *mens rea* (a guilty mind) component to be proven.[76] In a tort case, it is the consequences of the (in)action of the defendant which is examined, not their intent.

75 Joan Goodchild, 'The Botnet Hunters' *CIO* 2009 <https://www.cio.com/article/2422690/the-botnet-hunters.html>

76 There are a small number of exceptions, where certain torts require a specific intent, but this is not the case for the tort of Negligence which is the basis of the proposed framework.

Specifically, the framework applies the principles of Negligence, which is the breach of a legal duty owed by the defendant to the plaintiff and the consequences of that breach result in harm accruing to the plaintiff.

However, a fundamental principle of the proposed framework is that it can not be used to open the floodgates for malicious or vexatious litigation and nor is meant to allow for damages to be sought from every failure of cybersecurity. Instead, the framework has been written to provide clarity to software developers so that they can make a choice to incur the extra expense to adhere to the minimum standards required that will protect them from litigation subsequent to a cybersecurity breach or they can make the decision to not apply the standards and run the risk of litigation.

There are well settled principles of negligence,[77] and in order for negligence to apply, the following points must be demonstrated:

- The defendant must have a duty of care to the plaintiff
- The defendant must have breached this duty of care
- There must be sufficient causation, in the eyes of law, between the breach of the duty of care and the damages which subsequently arise.

The framework proposes the following:

- A vulnerability is discovered within the application or within a library which the application uses; and
- This vulnerability must be exploitable; and
- This vulnerability must have been exploited by a third party to enable the ensnarement of the device into a Botnet; and
- The developer must either be aware of the vulnerability or should have reasonable been aware of it; and
- The developer must have failed to develop and deploy a patch to remedy this vulnerability within a reasonable period of time or has not developed a means to update the device post sale.

Only if all if these points are met, should a negligence claim be able to be brought. If the developer has produced a patch, but the consumer has taken actions to prevent its deployment (which is not equivalent to failing to action an update), liability should not attach to the developer.

The framework also requires that when a developer releases an IoT product, it will have both a set Long Term Support (LTS) duration and a clear action which takes place once the LTS has been reached. This proposal is based on a modified principle outline by Bruce Schenier that an IoT device should 'fail predictably and safely'.[78] This proposal should be welcomed by developers as it removes the threat of an obligation on the developer of the software to maintain the security of the device *ad infinitum.* Instead, security patches will be required only for a reasonable number of years, which will be known to both the product manufacturer (to allow for planning) and consumer in advance of their purchase. The options presented to the consumer surrounding the device once it surpasses the LTS date should be similar to:

77 See, for example Richard A Buckley, *The Law of Negligence* (4th edn, LexisNexis 2005).
78 Schneier (n 53) 108.

- The IoT device will lose its Internet access and other forms of connections, becoming a 'normal' device
- The consumer can purchase additional security updates which will extend the LTS
- The developer can take no action, and thus risk becoming liable for any damages which arise following a cybersecurity failure

From a Botnet perspective, the aim of this model is to alter the behaviour of software developers so that once an exploitable vulnerability becomes known, developers will have the infrastructure in place to determine if the vulnerability applies to them, and if so, will develop a patch and deploy it. This will have consequence of making it more difficult for Botnets to recruit new nodes and to prevent the Botnet from leveraging a particular vulnerability.

It is very important to note that nowhere in this proposal is it suggested that software developers should be held accountable for the fact that a third party has breached the security of their software, but only when that breach was foreseeable and preventable. The common law system has extensive experience in assessing the negligence claims brought by plaintiffs who assert that their health has been damaged by the (in)actions of the defendants. Health cases are an excellent corollary to cybersecurity cases because when evaluating risks to health, the courts do not expect that risk is removed, but rather it is reduced to an acceptable level. These principles are outlined well in *Wilkes v. DuPuy*,[79] and *Hastings v. Finsbury Orthopaedics Ltd & Stryker UK Ltd*,[80] and demonstrate how the civil liability is able to determine causation in complex, multi-faceted situations which require extensive specialist knowledge and where obtaining absolute certainty as to causality is impossible.

From a technical perspective, this will mean that developers will not be responsible for zero-day exploits nor exploits which have not been reported to cybersecurity industry, and when an exploit becomes known to a developer, there will be a reasonable length of time for them to develop, test and release the patch. It is proposed that 'reasonable' in this context equates to ninety days.

4.2 Regulator Action

Although a regulator is not required for the proposed framework, the outcomes can be improved by certain regulator actions. One risk to the proposed framework is that there is a potential for market failure to occur as large companies, who are the usual victims of DDoS attacks may not wish to take an action against a consumer who failed to apply a security patch to their Smart Device. Accordingly, the framework can be buttressed by having a regulator identify and engage with consumers who own vulnerable devices instead of waiting for the legal action. Furthermore, there is scope for a regulator to oversee the interaction between cybersecurity researchers and software developers to ensure that vulnerabilities are acknowledged promptly. These actions do not overlap, and it is not envisaged that the regulator would play an active part in instigating the legal action at the heart of this framework. As such, the responsibilities can be apportioned out to existing regulator bodies or could be outsourced to independent bodies overseen by national regulators or supra-national organisations such as ENISA.

Recent work has focused on examining individual IoT devices to determine if they are vulnerable to attacks and has determined that such an assessment is quite feasible. Kim et al. (2018) propose a model which is based on ZMap, an open-source tool which seeks out IoT devices by searching IP

79 [2016] EWHC 3096 (QB)
80 [2019] CSOH 96

addresses and determining if the software has known security vulnerabilities.[81] This is similar to tools such as Showdan, Censys and ZMap, and applies analysis similar to that of Shovat.

The output of the model suggests a role for a regulator, as they will be able to obtain, within their jurisdiction, a complete range of IP addresses from all ISPs under their remit and could apply the tool to these addresses. Vulnerable devices can then be linked, via their IP address to an ISP account, whereby they can be 'put on notice' that they are running a vulnerable device, and the consequences of not updating the device would be to render them liable for damages if their device was used in a Botnet to conduct a cybercrime. It is important to note that the regulator (or responsible body) would not be provided with the personal details of the device owner, and it is not expected that the ISP would be responsible for performing the analysis.

This type of analysis lends itself to regulator activity as it can be automated, and a record of such 'notifications' can be maintained and can be used in civil suits. ISP involvement in preventing Botnets has been discussed in academia before, but unlike work such as Chandler (2006),[82] and Anderson et. al. (2008),[83] who recommend that liability (at least in part) attach to ISPs, this is not proposed in this model, partly because work such as Dupont (2016),[84] and Fryer (2013),[85] who demonstrate how cooperation between either large private actors or regulators and ISPs results in better outcomes then forcing liability upon them and also because the nature of the model is to foster choice for both developers and users to decide if they want to secure their devices and apply the consequences for those who chose not to. This work demonstrates yet again the robustness of the informal lines of communication which exist between the networks of cybersecurity practitioners and other relevant parties such as ISPs and software developers. Furthermore, it has been demonstrated that when entities have attempted to outsource enforcement requirements to ISPs, this can result in further legal between these parties which is an outcome which hinder the underlying intention.[86]

However, the provision of timely patches, as proposed by the model, still runs into the problem as outlined by Schneier (2018) who cites the well known adage that "one quarter of people patch on the day its released, one quarter within a month, one quarter within a year and one quarter don't patch at all".[87] These figures relate to computers, where the user is actively using them on a regular basis – for smart devices which lack a GUI and require a manual update (such as most household routers), it is reasonable to assume that a 25% patch rate would be an exceptionally good response. Therefore, a 'nudge' by a regulator to notify users of now-insecure devices would support the model and ideally also influence the purchase decision when the consumer is next buying a smart device.

An analysis of the proposed framework does outline a potential issue, which may be solved by the presence of a regulator. If, as proposed in the framework, firms are not liable for unknown vulnerabilities, it may incentivise them to act in a manner which makes the reporting for vulnerabilities difficult. This should only be an issue where a vulnerability has been found in a particular IoT device's software, and not in a third party library or component which is used by the IoT device. This is because such exploits are usually reported to third party databases when they are discovered by researchers or cybersecurity professionals. The most commonly used,

81 Hwankuk Kim, Taeun Kim and Daeil Jang, 'An Intelligent Improvement of Internet-Wide Scan Engine for Fast Discovery of Vulnerable IoT Devices' 2018 10 Symmetry 151

82 Jennifer A. Chandler, 'Liability for Botnet Attacks' 2006 5 Canadian Journal of Law and Technology

83 Ross Anderson and others, *Security Economics and the Internal Market* (2008)

84 Dupont (2016), n(3)

85 Huw Fryer, Roksana Moore and Tim Chown, 'On the Viability of Using Liability to Incentivise Internet Security'

86 See, for example *Mircom and Golden Eye v Virgin Media* [2019] EWHC 1827 (Ch); and *Twentieth Century Fox & Ors v BT* [2011] EWHC 1981 (Ch).

87 Schneier (n 53) 36.

according to Sánchez, De Gea, Fernández-Alemán, Garcerán and Toval (2020),[88] is the MITRE Corporation's Common Vulnerability and Exposure (CVE) database which is a free and open-access resource.[89] However, when a researcher or cybersecurity professional attempts to contact a developer directly with the news that they discovered a vulnerability, their communications may be ignored. Van Gastel and Meijer (2020),[90] outline the challenges which they faced when trying to report a vulnerability which impacted most solid-state hard drives produced at the time of their publication. They also relied upon a third party intermediary who was known to the manufacturers and who was able to protect their identities so as to ensure prevent the risk of law suits issued by the manufacturers.

In order to prevent such an outcome, a national regulator could act in a similar role to the intermediary. In a similar manner to how the CVE database has 'CVE Numbering Authorities' who are empowered to raise a CVE ID for a vulnerability, the regulator can appoint bodies who either 'copied in' on submissions to a manufacturer alerting them to a potential vulnerability or can be a point of contact if the vulnerability is ignored. It is envisaged that many companies would outsource the reporting management to third party specialists. It is important to note that the regulator should not be seen as the 'arbiter' of whether a vulnerability is material or not, but instead they act more as a record of reports so that a development company is unable to reduce the scope of their liability by delaying the recognition of a vulnerability or by choosing to ignore vulnerability reports, in the event that an action is taken against them.

5.1 Barriers to the New Framework

It is currently not possible to introduce the proposed new framework, without legislative action to remove a number of judicial and legislative barriers which would prevent a negligence action, as outline in this paper, from being brought before a court. A detailed examination of these issues are outlined in Nash (2020),[91] and a summary of them will be presented here, along with other non-legislative objections.

5.2 Pure Economic Loss

In order for liability to attach in a tort claim, the damages which occur must be either physical harm or property damage. It is possible that a Botnet attack results in damage to a person or damage to their property, but it is much more likely that the damage would be pecuniary, which is classified as *Pure Economic Loss*. This was clarified in *Spartan Steel*,[92] and remains in force today. The rationale behind the decision is a valid one – the courts did not want to become involved in every dispute where a party suffered a financial loss, as this would quickly lead to the swamping of the Courts with cases and a potential breakdown of the civil justice system.

However, there are strong grounds for why an exception to the doctrine should be made in the case of a negligence finding under the proposed framework. These grounds consist of that fact that is now eminently possible to calculate the direct costs associated with a cyberattack. If a consumer's device has been used, the 'wear and tear' cost of the extra usage can be calculated, while for the victims of the cyberattack, the direct costs (such as replacement infrastructure, cybersecurity consultancy costs, etc) can be calculated. There is also a strong argument that for businesses whose revenue has been disrupted by a Botnet attack, there are now

88 M. C. Sánchez and others, 'Software vulnerabilities overview: A descriptive study' 2020 25 Tsinghua Sci Technol 270

89 https://cve.mitre.org/

90 Bernarard van Gastel and Carlo Meijer, 'Hacking SSD's: How a Hobby Project Went out of Control' *Radboud Universiteit News* (29 April 2020) <https://www.ru.nl/@1268067/hacking-ssd-how-hobby-project-went-out-control/> accessed 28 September 2020.

91 Nash (n 5).

92 *Spartan Steel & Alloys Limited v Martin & Co (Contractors) Ltd* (1973) 27 QB (Queen's Bench).

sufficiently robust analytical packages to create a reasonable base-line estimate of lost trade. This is especially relevant for businesses whose revenue is asymmetric in nature and highly concentrated over a small number of trading days.

Until, however, either legislation is passed or a superior court breaks with precedence, the proposed framework will not be actionable due to the prohibition against bringing a Tort case where the nature of the damage incurred falls under the doctrine of Pure Economic Loss.

5.3 Products Liability Exceptions

Another challenge to the implementation of the proposed framework arises from the limitation in applying the principles found in Products Liability to digital products. For non-digital products, there is a well developed body of law which outlines how a consumer can bring a tortious action against a producer if the device imperils their safety or fails to work as intended for a reasonable period of time. Liability for defects generally moves along a scale, starting from strict liability, where the mere presence of a defect will warrant a return to 'normal' liability where the consumer will need to prove the defect.

Unfortunately for Smart Device users, digital products fall outside of the European Products Liability Directive,[93] and the 2019 EU Consumer Protection Directive.[94] As such, consumers who raise a claim against the product will need to demonstrate that there is a 'design defect' inherent in the code base.

However, a defence against such a claim for manufacturers is to demonstrate that, at the time of production, the defect wasn't known to be a defect at the time of production but only became apparent subsequent to the point of sale. While this makes sense for non-Smart Devices, the logic fails for Smart Devices as it is only once the device has been released that third parties will begin to study its operations and code for vulnerabilities. Therefore, in order to both introduce the proposed framework and to offer consumers, who are increasingly reliant on Smart Devices, the same level of protection they are granted for their 'dumb' products, a meaningful inclusion of Smart Devices and digital products is required.

5.4 Exclusionary Clauses

It is common practice for companies to include in their contracts or terms of service clauses which exclude their liability or limit it to a small or effectively nominal amount.[95] Exclusionary clauses, within the European Union are governed by the Consumer Rights Directive,[96] and the Unfair Terms in Contracts Directive,[97] a piece of legislation which dates back 1993 and as such, pre-dates the internet and the concept of Smart Devices. The Consumer Rights Directive sets out the requirements for the contract to be valid, but does not itself deal with exclusion clauses, which are dealt with in the Unfair Terms Directive.

Savin (2017) outlines in detail how the validity of the exclusion clause will be assessed,[98] but it can be generally defined as a term which has not been individually negotiated, does not relate to the price and is not of good faith which results in an imbalance in the rights and obligations to the consumer. As such, it should now be clear that there is a lack of clarity around the enforceability of exclusionary clauses in a consumer contract setting. This lack of clarity on the matter suggests that if a consumer was successful in bringing a negligence case against a

93 Directive 85/374/EEC
94 Directive 2019/2162/EU
95 Robert Bradgate, *Commercial Law* (Third Edition, Oxford University Press 2005) 263.
96 Directive 2011/83/EC
97 Directive 93/13
98 Andrej Savin, *EU Internet Law* (Second Edition, Edward Elgar Publishing 2017) ch 7.

producer, the producer would then seek to rely on the clause to limit liability or awarded damages, a foreseeable event which itself will act as a dampner on potential litigation being brought in the first place.

The success of such clauses could have a detrimental effect upon the proposed framework as it will severely reduce the downside risk to a software developer if action was brought against them which then could create a disincentive to maintain the security of their product. However, it is also important to note that although these exclusion clauses are ubiquitous in consumer software, these clauses aimed at excluding liability from consumer claims have never actually been tested in any senior court.[99] As such, they can be considered more as a statement of intent by the producers, as opposed to being enforceable contract terms. However, if the proposed framework is to be enacted, it is recommended that in order to ensure the avoidance of doubt, that a term be enacted which precludes the exclusion of liability arising from a failure to develop a patch for a known security vulnerability.

6.1 Conclusion

This paper proposes a novel methodology to disrupt Botnets, whose main principles can be summarised by Jagger and Richards (1969) who note that 'if I don't get some shelter ... I'm 'gonna fade away'.[100] If successful, the application of the proposed framework would create a hostile environment for Botnet operators, so that nodes which have been ensnared into a Botnet are less likely to remain within the Botnet over time, causing it to 'fade away'.

It should hopefully been made clear in this paper, there is no simple panacea in disrupting Botnets. Private individuals and companies, along with law enforcement bodies and cybersecurity institutions devote vast resources to disrupting Botnets and have recorded many successes. However, this paper highlights how as long as software manufacturers are able to keep producing IoT and Smart Devices which are shipped with default passwords and aren't maintained so that security vulnerabilities are patched, scalable methods to disrupt Botnet on an efficient basis will be a Sisyphean task.

Accordingly, the framework proposed in this paper aims to influence both the developers of software and the users of Smart Devices to incorporate cybersecurity into their respective expenditure plans, by using the threat of litigation to alter behaviour. If such an approach can be implemented, it will strengthen the hand of cybersecurity practitioners and it will implicitly enjoin the producers of Smart Devices into the action taken by entities such as Microsoft's Digital Crimes Unit, as their findings will result in deployed patches.

Finally, a benefit of the proposed framework is that, unlike multi-jurisdictional law-enforcement actions, the framework only needs to be deployed in markets such as the United States or the European Union. The size of these markets will require the developers to create the infrastructure to identify vulnerabilities, prepare remedies and deploy them. It would be economically efficient for these patches to only be deployed within the relevant market as this would require further expense and so, the legal framework within one or two large markets can result in global patching. A globally coordinated change to product liability and negligence is not required for a global effect.

The framework also has articulated methods which can be quantitatively assessed to determine the impact which it is having on the Botnet environment, as well as assessing the

99 Ian J Lloyd, *Information Technology Law* (Ninth Edition, Oxford University Press 2020) 426.

100 Mick Jagger and Keith Richards, *Gimme Shelter* (Olympic Studios 1969) <https://www.youtube.com/watch?v=QeglgSWKSIY> accessed 6 September 2020.

'quality' of Botnets following its imposition, which can be used by the suggested regulators to target the vulnerabilities which will have the largest impact disrupting Botnets.

The author of this paper is not naive enough to believe that the proposed approach can simply be rolled out without strong push back from the Smart Device industry, but takes heart from the sentiment as outlined by Jagger and Richards (1969) '*You can't always get what you want, but if you try sometimes, you get what you need*'.[101]

101 Mick Jagger and Keith Richards, *You Can't Always Get What You Want* (Olympic Studios 1969) <https://www.youtube.com/watch?v=EJRdDhnTRoo> accessed 15 October 2020.