Collective responsibility and mutual coercion in IoT botnets
A tragedy of the commons problem

Carolina Adaros Boye[1], Paul Kearney[1] and Mark Josephs[1]
[1]*Birmingham City University, B4 7XG, Birmingham, UK*
carolina.adarosboye@mail.bcu.ac.uk, paul.kearney@bcu.ac.uk,mark.josephs@bcu.ac.uk

Keywords: Internet of Things, DDoS, botnet, Mirai,The Tragedy of the Commons, Cyber Security

Abstract: In recent years, several cases of DDoS attacks using IoT botnets have been reported, including the largest DDoS known, caused by the malware Mirai in 2016. The infection of the IoT devices could have been prevented with basic security hygiene, but as the actors responsible to apply these preventative measures are not the main target but just "enablers" of the attack their incentive is little. In most cases they will even be unaware of the situation. Internet, as a common and shared space allows also some costs to be absorbed by the community rather than being a direct consequence suffered by those that behave insecurely. This paper analyses the long term effects of the prevalence of a system where individual decision-making systematically causes net harm. An analogy with "the tragedy of the commons" problem is done under the understanding that rational individuals seek the maximization of their own utility, even when this damages shared resources. Four areas of solution are proposed based on the review of this problem in different contexts. It was found necessary to include non-technical solutions and consider human behaviour. This opens a discussion about a multidisciplinary focus in IoT cyber security.

1 INTRODUCTION

Botnets are considered to be a significant cyber security threat (Mansfield-Devine, 2016). The typical mechanism consisted on taking control of a number of computers which are known as bots or zombies used for different purposes such as sending spam, performing distributed denial-of-service attacks, harvesting user credentials, committing financial fraud, hosting phishing sites, or performing click fraud on advertising networks (Asghari et al., 2015). In the past years a new modality of botnet has become frequent which uses insecure IoT devices to perform Distributed Denial of Service (DDoS) attacks to a third party. This sort of attack takes advantage of the fact that IoT devices are growing in number and many of them have an insecure design or are configured insecurely. Also, most of them are kept connected 24x7 and left unattended.

In 2016 two consecutive DDoS attacks were registered that involved a malware called Mirai. This malware consists on a set of exploits that search for insecure devices in the internet taking control of them to build a botnet. Mirai works sending TCP SYN probes to large numbers of IP addresses to scan for vulnerable devices and attempt to establish a connection through dictionary attacks using a list of 62 typically used default credentials. After each successful login the IP address and corresponding credentials are stored in a server and a separate program is used to download and execute the malware in the device, enabling communication with the command and control platform (Antonakakis et al., 2017). Once this is done, the attacker can send commands to the devices making them send connection requests to the target victim. The first attack was in September 2016 and the victim was the web-page of Krebs on security. The second attack was in October and it has been one of the biggest botnets ever registered. The victim was the DNS service provider Dyn and the attack affected several of its clients in Europe and USA including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

The code of Mirai has been made publicly available and a number of variations have been developed, targeting IoT devices from different brands which have a Linux-based OS. This makes it a latent threat at the present. Furthermore, Mirai attacks have been launched the past couple of years to several targets including Deutsche Telekom, game servers and other sites (Antonakakis et al., 2017). It has to be noted that this is not the first malware designed to perform this

sort of attack. Another example is Bashlite which also infects a variety of systems that use Linux.

According to the report released on March 2018 by F5 Labs, there is evidence pointing towards IoT devices becoming the attack infrastructure of the future (Boddy and Shattuck, 2018). This is not surprising since it is expected that the amount of connected devices will continue to grow (Gartner, 2017) and new threat actors and attack mechanisms are continuously arising (Boddy and Shattuck, 2018). Figure 1 shows that there was an important increase of telnet attacks since the development of Mirai with a peak at the beginning of 2017.

The analysis done on this paper will be mostly based on Mirai botnets, but this does not mean that the approach cannot be useful to study other threats to IoT or to be applied to other cyber-security problems.

One remarkable thing about the infection of IoT devices with Mirai is that, in theory, they are fairly simple to avoid. It is only required to change the default password. Also, if the device is already infected, it can be cleaned by rebooting the system to erase the malicious code. Then, the password needs to be changed to avoid it getting infected again. This is very likely since the rate of infection of Mirai has proven to be in the order of the hundreds of thousands of devices per hour (Antonakakis et al., 2017). However, in practice, changing the password, might not be easy or even possible, even though it should be considered a basic hygiene measure. For example, it was detected that, many of the devices involved in the Dyn attack were from a specific electronics manufacturer who had the credentials hard-coded in the firmware, making them unfeasible to be changed (Krebs, 2016a). Also, even in the case of devices that allow changing the password, there is currently no practical way to ensure that the device owners do it.

This paper makes use of a well-studied economic predicament named as "the tragedy of the commons" to make an analogy with the problem of the IoT botnets from a non-technical perspective. The fact that manufacturers and users are neither motivated nor compelled to improve their security was the main driver for doing an analysis from a social behaviour prism. The idea is to develop a better understanding of a scenario where the benefits are distributed individually and the costs are shared by a community and to discuss potential solutions. The main points in which the analogy is based are explained in section 2. Section 3 reviews previous work done where "the tragedy of the commons" is referred in the context of availability and cyber-security problems, including botnets. Sections 4 and 5 suggest possible solutions, and section 6 provides the conclusions and recommendations for further study.

2 BOTNETS AS A "TRAGEDY OF THE COMMONS" PROBLEM

The tragedy of the commons is an economic problem which was for the first time addressed in 1833 by William Foster Lloyd (Lloyd, 1833) who exposed what has become a well-studied economic problem. The "commons" where shared areas where herd belonging to different owners could graze freely. Therefore while each owner had a benefit that was proportional to the number of animals they owned, the costs of feeding them would be shared by all the herdsmen in the common. As long as the common is big enough to feed all the animals (as well as having a buffer for regeneration) there is no problem. However, each member of this community, as a rational decision maker, will try to maximise their utility by increasing their number of animals. Eventually this will reach the point that the common, having finite resources, will not be sustainable to feed all the animals. In 1968, Garrett Hardin published a paper under the name The tragedy of the commons using an analogy of this problem to analyse overpopulation (Hardin, 1968). Hardin also introduces an in-depth analysis of situations where individual decisions, which are based on pursuing personal gain, can affect the common interest and explains. In other words, how the benefits of a few can cause detriment to a community.

When the rules of the game are established in a way that rational individual decisions harm the society as a whole, the only possible solution is to change the rules. Furthermore, Hardin introduces the idea that certain problems have no optimal technical solution, for which, in certain scenarios, to preserve freedom there is a necessity to establish laws and regulations. This is based in a basic economic principle that establishes that the needs are unlimited but the resources of the planet are not. Another example used in this same publication is the damage to the environment where companies and individuals, as a consequence of activities that mostly benefit themselves harm the ecosystem through pollution. So this is also a case where the benefits are individual but the costs are shared.

According to Hardin 's essay, the tragedy of the commons has two, fairly equivalent, scenarios, the first scenario is when individuals extract something from the common resource compromising its availability, and the second scenario is when the individuals introduce something harmful to the environment.

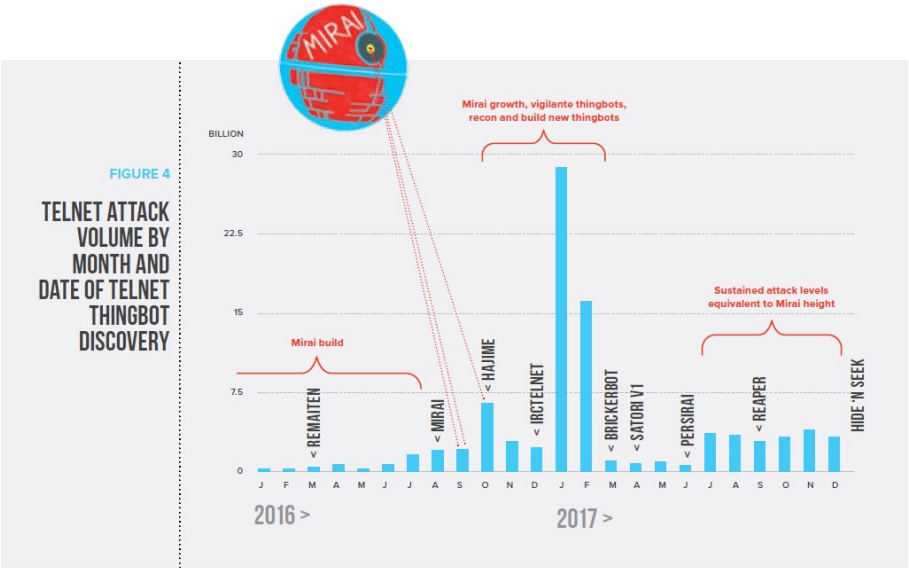

Figure 1: Telnet attack volume by month according to F5 Labs threat report (Boddy and Shattuck, 2018)

In this paper, it will be explained how in the cyber space, this problem can be seen from both sides, by using the particular case of IoT botnets. On one hand, the cyber space is based on a physical infrastructure that is limited and therefore its availability depends on this limit not been reached. On the contrary of what some could intuitively think, the major constraint is not related to the capacity of the channels but to the processing limitations of network devices, such as routers. Another problem that affects availability is the not optimal use of the routing resources and channels (Lutu and Bagnulo, 2011). (den Hartog et al., 2017)(Cole et al., 2006). On the other hand, users can either, maliciously or unknowingly, introduce pollution to the network such as hurl traffic, and malware (Cerf, 2013).

In general, availability issues are not frequently applicable for the normal use of internet due to its ability to increase its capacity in respond to demand. Nevertheless, in certain cases, traffic congestion levels can result in the unavailability of a service for certain period of time(Cerf, 2013). This is the main principle of a DDoS attack. In an IoT botnet also malicious traffic is injected to the network making a clear parallel with the pollution example since the misuse of the internet leads to increase different risk factors in the environment, making it insecure for all the users. This last applies not only to botnet malware, but also to all sorts of malicious activity. If all the security efforts are focused in the malicious agents that launch the attacks, and in the main victim, we are forgetting important actors who enable the attack. In the rest of this paper, these actors will be called “enablers” or “botnet enablers”. These actors are a key part of the success of the attack, meaning that they could also be key in preventing it, or stopping it. For this, it is important understanding what drives their actions. The case is that “botnet enablers” will not intentionally mean to provoke harm. They just limit themselves to seek the maximisation of their own utility, which usually is a natural human behaviour.

There will be three types of actors considered as “botnet enablers”: the IoT manufacturer, the IoT owner, and the Internet Service Provider (ISP). Each one of these three actors would try to maximise their utility function by reducing their costs.

The IoT manufacturer would be allegedly the actor that has the main responsibility since is the one producing an unsafe device in the first place. The IoT devices susceptible to attacks based on Mirai have the characteristic of allowing software to be downloaded and installed without requiring higher level privileges. Also not only they do not enforce changing default passwords, but a particular brand that was involved in the two big cases of 2016 did not even allow the user to change it because credentials were hard-coded.

The second actor, the IoT owner, represents the roles of administrator and user. The IoT owner also enables the attack by performing selfish actions which are in the first place, purchasing an insecure device, by connecting it directly to the internet without any network protection, and by not changing the default credentials (in the cases that this is possible). In the ideal situation, the user should have as little freedom

as possible to behave insecurely which is achieved by having security by default and privilege separation. Users will often lack security awareness and it should be responsibility of IoT vendors to provide guidance.

The third actor, the ISP, despite not having legal obligations towards security, several security experts agree that they are in a suitable position to protect the internet (Usman, 2013). Therefore it is believed that it should become a common best practice that ISPs have responsibility for traffic coming from their network, and this includes IoT-bots (Smith, 2017).

Not having the knowledge or the technical capabilities for playing their part in avoiding a DDoS attack of this scale can be at some extent an excuse (or maybe not) for the "enablers". This would bring a fourth player to the game which is the type of actor that is called to help solving both the awareness and the tragedy of the commons problem: regulatory entities. This includes industry standards, as well as market, and legal regulations. If the regulatory entities only focus on the attacker and ignore the role of the "botnet enablers" it will be an endless quest since they will be missing out the big picture.

Finally there is a fifth actor, which is the victim. Basically the victim is all the internet community. This includes the direct victim of the DDoS attack, as well as everybody that is affected directly or indirectly for the lack of availability of their services. Figure 1 shows a diagram with the different actors and their current roles in a DDoS botnet of the type caused by Mirai.

So lets see how the different elements involved in a botnet relate to the tragedy of the commons problem by doing the following analogy:

- **The commons:** they are a shared space in which the actions of individuals affect either the availability or the quality of the resources in it. This corresponds to the cyber-space which clearly has the characteristic of been susceptible to be affected in its availability and quality of service by individual decisions of its users.
- **The herdsmen:** they are the individuals that share the commons whose decisions have an effect in the community as a whole. As much as they get affected themselves, as this effect is shared between the members of the community, the herdsmen will not always perceive the harm as a direct consequence of their actions. And even if they do, they will not have the necessary incentives to change their behaviour. In this case, the herdsmen are the "botnet enablers" which are the first three actors: the manufacturer, the IoT owner, and the ISPs.
- **"Grazing cattle":** is the action of making use of the common space. This can be done either in a sustainable or in an abusive way. It would be consider sustainable when the resources are far to reach their limits in the foreseeable future or when there is a sense of collective responsibility to preserve the resources of this space. As this sense of "collective responsibility" cannot always be guaranteed for all individuals, different sorts of incentives and deterrents can be allocated to compel the herdsmen to limit their number of animals. It is understood that "limiting the number of animals" represents having a responsible behaviour towards the sustainability of the resources.

When the herdsmen are free to graze their cattle as they wish, they will try to maximise their own utility in detriment of the commons good which is the preservation of the resources' availability and quality. The scenario of grazing cattle in a sustainable manner represents making use of the cyber space in a secure way. In the botnet example, this means manufacturing, deploying, and using IoT devices securely, plus ongoing monitoring and control of network traffic in the Internet. All of which can be done by the different "botnet enablers". The scenario of grazing cattle in an abusive manner is the one that allows the development of the botnets. The omission of actions to prevent the IoT devices getting infected and used as bots, presuming that this will not have any direct consequences, could inflict as much damage to the community as the malicious action itself.

On a nutshell, there are two main characteristics of the IoT DDoS botnets, namely botnets based on Mirai, which support doing the analogy with the tragedy of the commons. First that there is a space that is shared, and so are the resources that this space offers. Second, that individual decisions made with the goal of maximisation of the utility function of each stakeholder is opposed to the goals of the common good. In this case, keeping the internet as a safe place is considered to be for the best interest of society, reason why cyber attacks are considered among the most relevant risks that humanity faces at the moment (World Economic Forum, 2018). So the whole society is the one that suffers as a consequence of too many individuals ignoring their social responsibility.

Two actors in the botnet that are not considered explicitly in the tragedy of the commons analogy are the perpetrator of the attack and the direct victim of the DDoS. In the case of the attacker, since this player is not likely to follow any rules, he is not invited to the game. On other words, there is no control over their actions. So for the scope and purpose of this analysis the attackers behaviour will be assumed as constant rather than variable. The direct victim, although not

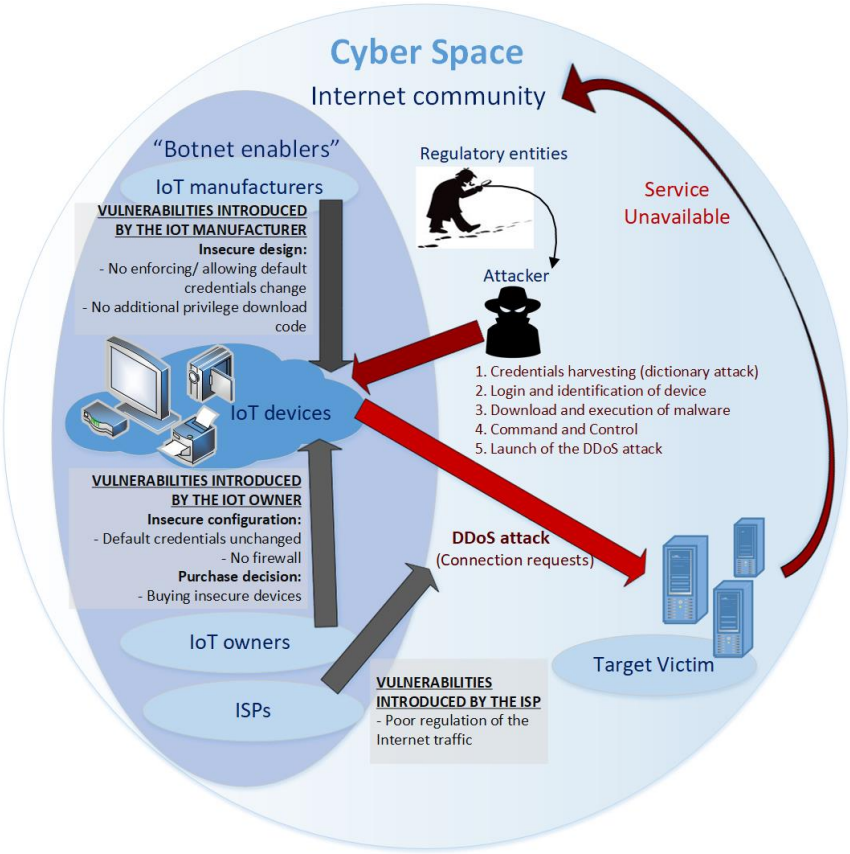

Figure 2: Roles and responsibilities of different actors in a Mirai IoT botnet.

explicitly represented, they belong to the fifth group of actors: the community. This actor constitutes a particular case, which might require a separate subdivision in a future expansion of this model, since in a single event they will be paying a much bigger proportion of the costs than the rest.

It has to be noted, as well, that as much as the last actor was named as the internet community, actually there is an increasing amount of services that rely on IT that serve people that might not even use internet, such as elderly people. Banking, health-care, utilities, retail, and public services are example of services that highly depend on IT. On other words, a denial of service can affect mostly any ambit of human endeavour and this dependency should be expected only to increase with the boom of IoT and industry 4.0. In the long run, everybody will suffer the consequences at some extent. If not in the next botnet, in the consecutive or at some point in the future. It is just a matter of big numbers and probabilities, in which having this situation going on for an extensive period of time makes likely that, at some point, every member of the community will become a victim.

According to this, for a period of time "t" we could consider the following statement to be true:

If $(t \rightarrow \infty)$
then,
The total costs of DDoSs will be distributed among all Internet users

This is rather theoretical and probably in a finite period of time the share of the consequences of a botnet will never be equal among all members of the community. To make a consensus, we can agree that in the long term, most members of society will at least suffer some sort of consequences, although these will not be equally distributed. While cannot demonstrate an equal proportion of consequences among the community, we can still agree that the actors whose decisions can make the difference are not significantly affected by the DDoS in a different way than any random member of the community. Actually, an experimental study done to estimate the cost for an individual IoT owner to have their devices infected by Mirai and used as bots in a DDoS attack showed these

costs are negligible (Fong et al., 2018). The analysis demonstrated that while the overall cost for these actors as a whole was significant, the costs for each individual IoT user was not that big, and could easy remain imperceptible by them. They estimated 1.08 USD of cost per device in the attack against the Krebs on security website and less than 0.01 USD. This corresponds to a direct cost which is electricity consumption. They estimated also a higher cost attributable to bandwidth consumption, but this is usually not directly payed by owners since it is very common to have unlimited broadband contracts. So again the whole community is the one that absorbs this cost.

Other consequences for IoT owners such low performance of the device can be harder to measure and were not included in the study just mentioned. It has to be taken in consideration that many users might not even notice issues with performance, especially if they are not using the device at all moments during the attack. And even if they did, this does not change the fact that this impact is out of proportion compared to the overall damage.

The unintended damage caused by the "botnet enablers" could be also defined as "economic externality" which is a direct effect of the activity of an actor on the welfare of another (Asghari et al., 2015). This is what can happen when in an interconnected world free agents make selfish decisions. DDoS botnets produced by bots hosted in IoT devices threaten to be a prevalent issue with the continuous growing trends of the IoT market (Gartner, 2017). This means that if no practical and widely applicable solution is implemented there are chances that this will be an increasing problem.

There is apparently no technical solution to ensure that the appropriate preventative measures are put in place, which is one of the characteristic of the tragedy of the commons dilemma. The typical conclusion that is reached in these cases is that there is a need for other nature of solutions (Hardin, 1968). It could be argued that, technically, it is very easy to prevent an IoT device to get infected with Mirai: having a secure password. Also, to clean an already infected device it is a matter of rebooting it and changing the password. But the real problem relies in the lack of incentives for owners to do this and, even more important, for manufacturers to build security by default (e.g. enforce a secure password). Therefore we are facing an economic and social problem which needs to be tackled as such.

The "botnet enablers" perceive no benefit from an attack, as the herdsmen do by exploiting the commons. But the tragedy of the commons is not always about benefits but about maximising the utility function, which is what rational decision makers tend to do. This does not mean necessarily to obtain a benefit, but can be also to avoid a cost. Taking action to avoid a botnet has a cost for all the three enablers. Even if for the IoT owner the cost is just some minutes of their time, they do not see any benefit in doing so. If they also happen to own a device that does not allow to change the default password, then the responsible action would be getting a more secure one. In this case the cost of security would appear to be bigger for this actor. Of course, this is only in the case that they knew the risk of connecting an unsafe device in the first place.

Another factor that matters in this problem is awareness. Not necessarily all "botnet enablers" are in purpose causing damage. There is a question here related to what if creating awareness and educating in the matter will result on them making a different decision making process. This is another issue that is covered in the tragedy of the commons analysis done by Hardin. He states that "education can counteract the natural tendency to do the wrong thing", but he also explains that this is neither a definitely nor can be the only solution to this sort of problem. It is of common knowledge that, once given all the relevant information, some people will act in a responsible way, but others will not. In the second case is when incentives, deterrents, and coercive measures are brought to the conversation which will be discussed further in sections 4 and 5.

3 CYBER-SECURITY AND THE TRAGEDY OF THE COMMONS

To the best of our knowledge, this is the first academic paper that analyses IoT botnets explicitly from this angle. Nevertheless, the idea of a link between IoT botnets and the tragedy of the commons problem has been suggested in some articles written shortly after the high coverage of the Mirai attacks of 2016 (Smith, 2017)(Krebs, 2016b). Also a number of published papers (Roy et al., 2010) (Herley and Florêncio, 2009) and articles (Cerf, 2013)(Iannela, 2017)(Davidow, 2012) relate this economic and social dilemma with cyber-security.

While the overuse of the internet is not a typical scenario of the tragedy of the commons, a limited number of papers have been written relating it with network traffic (den Hartog et al., 2017)(Lutu and Bagnulo, 2011)(Cole et al., 2006). In this case, more than bandwidth, the resources that appear to act as a bottleneck are network devices such as routers, which have limited processing and memory capabili-

ties (Lutu and Bagnulo, 2011). Also anarchy in routing (Cole et al., 2006) or in assignation of Wifi channels (den Hartog et al., 2017) is a cause of these bottlenecks. In neither of these cases the individual decisions are motivated for a gain but rather for avoiding the cost of investing energy to reduce entropy levels. The solutions proposed in these cases were related to algorithms for collaborative channel selection (den Hartog et al., 2017) and to introducing a tax mechanism (Lutu and Bagnulo, 2011). While the first approach appeals to a sense of collective responsibility, the second introduces a deterrent to prevent an unwanted behaviour. What both cases have in common is that they solved the problem by introducing new rules to the game in order to motivate a change in individual decisions. If the application of deterrent measures such as paying royalties, fines or taxes is agreed within the community for the greater good, this is called "mutual coercion" (Hardin, 1968).

An important issue yet to be solved in cyber security is the allocation of incentives and deterrents among the stakeholders that are well positioned to apply defence measures. Speaking about botnets, criminal incentives are only one side of the problem and the other side is that there is no incentive for defenders (Asghari et al., 2015). This lack of incentives is the same that makes the utility function of the IoT owners to remain almost the same either the take or not action. Therefore, leading them to do nothing, which is at the end some sort of decision. A decision that has consequences for society as a whole. Generally speaking, poor security levels in IT and IoT systems have a social cost, due to the fact that most of the society benefits one way or another from the ICT ecosystem meaning that cyber-security has similar characteristics of a public good. The problem is that the fact that defences are put in place mostly as a decision made by privates (e.g. individuals and companies) provokes that costs and benefits are not evenly distributed among the different actors (Bauer and Van Eeten, 2009). When an actor does not directly perceive all the consequences of their choices cyber-security problems become more complicated. Therefore, this asymmetry is an important cause of this tragedy. And it is not just the problem of availability but that this situation can lead to the risk that at some point the internet could become too unsafe for reliable use (Cerf, 2013).

The consideration of the economic and the human factor in the search of cyber security solutions is based on the fact that technology has no moral value by its own but it reflects human intentions having the power, as well, to amplify them (Iannela, 2017). Botnets are, in fact, a good example of using technology to amplify a malicious intent. It is then necessary to find the means to facilitate collaboration within different actors to counteract this situation, concerting efforts within the public and private sectors, including legal measures, if necessary (Bauer and Van Eeten, 2009). The literature suggests that the tragedy of the commons analogy, as well as game theory can be promising in providing perspectives, insights, and models to address cyber-threats (Roy et al., 2010).

4 COLLECTIVE RESPONSIBILITY VERSUS MUTUAL COERCION

In October 2016 an US senator who also called the Mirai botnet a tragedy of the commons problem expressed his worry that in this case security which is "so vital to all internet users remains the responsibility of none"(Krebs, 2016b). It is important to notice that speaking of collective responsibility can imply that it is everybodys problem but, at the end of the day, nobody is accountable for it. This would be like a famous Spanish play called "Fuenteovejuna" where a whole village takes blame for a murder to cover the murderer. The idea behind was that if the fault was committed by the whole village, nobody would pay the consequences. In the case of an IoT botnet the "murder" is, indeed committed by the village of the "botnet enablers". It is true that they are mostly guilty by omission rather than by action and it appears as quite unfair to attribute the condition of "criminal" to these actors, for been merely unintentional enablers of a cyber-crime. But what if they knew about the risk? Can we still defend their cause as an unintentional sort of complicity with the cyber criminals?

So the first step for collective responsibility should be creating awareness of the role that each actor plays and what they can do to prevent a DDoS attack. This would mean to trust that, having all the facts, they will have no choice but change their behaviour, driven by moral principles. But Hardin does not totally supports this hypothesis in his theory. If we accept the analogy between the commons and the cyber space to be truth, then the security of the internet can no longer depend on self-regulation (Davidow, 2012). Knowing that some components of the utility function of each actor are individual and others are shared the logical action would be to take concrete actions to balance the equation. The same as is in the case of solving overpopulation, environmental pollution, and the tragedy of the commons.

According to Hardin, "the social arrangements

that produce responsibility are arrangements that create coercion of some sort". Examples of this are taxes, payed parking spaces, and punishment for crimes. The validity of these kind of measures would be based on the agreement among the majority of the people affected (aka "mutual coercion"). This is because total freedom is not possible when this will affect the common good (Hardin, 1968). Another example of how individuals will not act against what they believe to be their self interest in favour of collective interest unless there is an explicit agreement is the prisoners dilemma. Taking this back to cyber security, it means that there should be some sort of agreement in place rather than having actors deciding independently. The ideal outcome of this agreement will be that manufacturing, selling, and connecting insecure IoT devices becomes intolerable.

The use of "altruistic punishment" can be demonstrated as an effective way to solve the tragedy of the commons dilemma through a zero sum game simulation experiment (Greenwood, 2016). Altruistic punishment means that some player will support the application of punishment to players that act against the common interest even if they do not perceive any direct gain for it and even if the punisher has to pay a cost. The reasons of this result is that the punishment acts as a deterrent and after a few rounds of the game the transgressors would change their behaviour.

Another interesting quote from Hardins paper is when he states that "the morality of an act is a function of the state of the system at the time it is performed". Therefore, as much as using a default password for a connected printer cannot be stigmatised as "immoral" by itself; how this changes if you know that it can be part of a DDoS attack targeting a critical service, such as a hospital?

Finally, the realisation that a resource is in danger reveals an urgent need for regulations to be put in place (Davidow, 2012). At the beginning of times, when the resource is safe from been corrupted and appears to be unlimited, there is room for freedom. There are several examples of this such as fishing, hunting, agriculture, environment pollution, and of course, the herd grazing in the commons. The internet seems no different to these other economic activities in the sense that it is becoming unsafe to be used freely (Cerf, 2013).

While several regulations are currently active related to behaviour in the internet including the recent enforcement of the General Data Protection Rules (GDPR) in the European Union, there is a lack of such regulations regarding IoT. Examples of concrete but isolated actions regarding coercive measures that involve IoT have been cases of smart toys forbidden in Germany in 2017 for threats to privacy and drug pumps pulled off the market by their manufacturer due to be found vulnerable to hacking. Similar measures should be taken regarding devices that are easily hacked to be used as bots.

5 POSSIBLE SOLUTIONS

The present paper does not aim to provide a definitive answer but to propose possible areas of solution. Specific ways to apply these solutions require to be developed in more detail, adding an in-depth analysis that takes in consideration the multiple disciplines involved. The fact that this is a complex problem that involves several actors, requires an analysis that includes the technological, economical, social, and legal points of view. It is suggested to integrate different types of solution rather than looking for some sort of silver bullet.

In order to provide material for further discussion, four areas of solution where identified, based on the premise that either consciously or unconsciously every rational decision maker will seek to maximise their utility function (Hardin, 1968). The four groups are: solutions that change the utility function, solutions that change the inputs of the utility function, solutions that involve coercive measures, and solutions that involve providing a better information about the variables of the utility function.

1. **Solutions that change the utility function:**
   This means introducing moral values to the equation by creating awareness about the problem and the major social implications, appealing to the consciousness of the different actors. Examples of this are doing campaigns that, one hand serve for education and, on the other, can make appear as "socially unacceptable" to connect devices insecurely to the internet.

   There are several examples of behaviours that were considered acceptable in the past, like throwing litter in the street or smoking inside a building which are currently no accepted anymore. This is also known as "blame and shame". Under this order of values, for manufacturers to produce an insecure IoT device would be the equivalent of selling toys with lead paint: not only a transgression to regulations but also a reason to appear in the newspapers. On other words, making a threat of serious damage to brand reputation could be used as a deterrent for "bad behaviour". Making public which vendors sell secure devices and which ones do not is another form of "blame and shame" or positive reinforcement, depending on the case.

2. **Solutions that change the inputs of the utility function:**

   These solutions imply introducing incentive and deterrents to change the utility value of the "enablers" in order to induce rational decision making. This should produce the same outputs that collective responsibility would, but it adds measures for assurance of "good behaviour". Examples of this are taxes, fines, or other sort of mutually coercive measures that add to the costs of the utility function of individuals. This can also be used as adding to the benefit part of the equation. For example by public recognition and good publicity for manufacturers that do "the right thing" as an incentive for secure design in IoT.

   ISPs besides been an actor themselves, can also be an agent of change of the utility function inputs by identifying device owners that have insecure devices connected and applying them a fine or additional charge in their service bill. This additional charge, in fact, would be totally justifiable in the sense that these users are in fact more costly for the system than the responsible ones.

3. **Solutions that involve coercive measures:**

   In this case, rather than trying to guide the actors behaviour by modifying their utility function, the solutions are oriented to put restrictions. On other words, they would be "compelled to do the right thing" by putting in place laws and regulations. For example, not allowing insecure IoT devices to be sold in the market.

   An extreme example would be to prosecute botnet enablers for criminal offence. An analogy to justify such a radical coercive measure is the case of a person that legally owns a gun and does not keep it in a safe place. As a result of this it is found by somebody and used to commit a crime. The owner of the gun will be certainly brought into justice and in the best scenario will need to provide a good explanation. In the worst, they will have to serve in prison. The situation is very clear, this person is facilitating the perpetration of a crime by been oblivious to a known risk. Therefore they have to respond for this. Then performing a denial of service attack is a crime, and IoT owners are enabling this crime.

   This solution points to, rather than making "enablers" collectively responsible for an attack, to make them individually accountable. Of course bringing hundreds of thousands of users around the world to a court will present some logistic problems, but maybe there are other possible measures that are less extreme like making them pay an extra fee for their internet service.

   ISPs also have an important role due to been well-positioned to regulate traffic and detect offenders, reason why some authors defend the idea to create laws that bring them into the chain of responsibility (Usman, 2013).

4. **Solutions that involve informing about the variables involved in the utility function:**

   This area of solution differs from the first one because it does not bring the moral speech to the table; it provides the decision maker with information about different variables that should be present in their utility function which might have been either omitted or miscalculated because of having incomplete information.

   If IoT owners are informed that it is a wrong assumption to believe that connecting insecure IoT devices to the network has no direct impact to them, they might change their behaviour. Actually, having insecure devices also exposes them to other threats such as data theft and ransomware attacks. For manufacturers, there can be also other consequences like been forced to take products out of the market and bad brand reputation. They also can have wider benefits if they can make an effective marketing campaign and build a reputation for selling secure devices.

   Trust of the customers should be considered as a valuable asset because consumers have the power to affect the market with their purchase decisions. Thus, IoT owners should be better informed about which brands are more reliable. To do this last bit, it will be necessary to have standards that allow developing some sort of labelling for IoT devices analogue to the one that domestic appliances have for power consumption efficiency. An example of this is the IoT Security Foundation User Mark which can be used by organisations that implement their latest security compliance framework (IoT Security Foundation,).

It must be considered that although some solutions and analogies might seem extreme, it is not meant to do a moral judgement of the so called "botnet enablers". The main purpose of the examples is to bring on a debate of how responsibilities could be assigned according to the capabilities of each actor to apply preventative measures. The only actors that actually have the intention to perform the attack, are the ones who infect the devices and launch the DDoS attack and, as it was explained in section 2, they were on purpose left out of the analysis.

While ISPs already offer DDoS mitigation services to potential DDoS victims amongst their cus-

tomers, they also could clean traffic of malware and hence help prevent infection. They could, as well, notify and provide support to owners of insecure IoT devices and sources of DDoS traffic and penalise those who, after been warned, do not disconnect or configure securely their device. For example, by extra charges.

The involvement of ISPs could present technical difficulties due to the need to process big amounts of data in near real time. Also, there might be constraints regarding privacy. Particularly, the General Data Protection Regulations of the European Union (GDPR) establishes conditions for consent regarding data processing (The European Parliament and the Council of the European Union, 2016). Possible ways to overcome these challenges are using advanced data analytics and that the internet consumers sign specific forms of consent for this purpose. Ideally, solutions should be oriented to look into suspicious characteristics in the heading, IP address, and size of the packages, rather than looking into the payload.

6 CONCLUSIONS

While avoiding an IoT botnet has fairly simple technical solutions, there is no simple way to enforce the relevant actors to apply them. The analysis presented in this paper does not see the botnet as a technological problem but as a behavioural problem. A "tragedy of the commons" approach can give clues of the nature of possible solutions, by studying how similar problems have been solved in other contexts such as over population, pollution, and network bottlenecks. Most of these problems have technical solutions that depend on the collaboration between different stakeholders which ends up becoming by itself a problem.

This analysis reveals that IoT botnets can be easily seen as an economic problem in the sense that different actors have the freedom to decide in favour of their individual utility even if this brings harm to the society as a whole. Therefore, there will be no realistic solution if human behaviour and economic principles are not taken in account. It is recommended to do a deeper study on the different areas of solution proposed and how it is the best way to combine them.

The solutions proposed are not meant to be restricted to control IoT botnets but also can apply to a number of cyber security issues and consider, as well, other risks introduced by IoT such as propagation of malware and privacy threats. Other actors should be considered such as Cloud and Software as a Service (SaaS) providers. The example developed is only an simplification of the problem to illustrate the analogy with the "tragedy of the commons" and to discuss how current cyber-security challenges can be faced introducing non-technical solutions.

Because it is known that people are the weakest link of the security chain, it should be understood that the amount of preventative measures that depend on the user should be minimised. The manufacturer should ship the products secure by default and provide appropriate guidance to users on how to connect and operate securely their IoT devices. Nevertheless, users still should be given the necessary information to develop, at least, a basic level of security awareness.

As humans are the cause of many cyber security problems, and not technology, human behaviour should be under consideration to find solutions for IoT security. It is, as well, important to consider a multi-disciplinary approach. The disciplines should include, but not necessarily be limited to the following:

- **Technology:** To create and implement technical solutions. This should consider different perspectives such as software and firmware design, hardware design, software and hardware integration, network security, cloud security, and physical security, in order to include all aspects of IoT.
- **Processes:** To identify key activities during development, deployment and operation where security aspects need to be considered. It is important to have experts that can identify the proper standards and sets of good practices, as well as security certification mechanisms.
- **Economics:** To understand how the market might react to the different types of solutions suggested, and to changes in consumers behaviours.
- **Human behaviour:** To understand the decision making process of individuals, what are their drives and what is the potential effect of incentives, deterrents, and coercive measures.
- **Law and regulations:** To define pertinent coercive measures and appropriate legal mechanisms for compliance.
- **Communication and marketing:** To spread the message in an effective way.

The introduction of mechanisms of "mutual coercion" appears like a plausible alternative to ensure that there would be accountability, not only for perpetrating a cyber-attack, but also for facilitating it. It has to be noted that coercion and education are not mutually exclusive. Enhancing security awareness is still an important issue to consider in order to create

consciousness in "botnet enablers" and induce them to adopt secure behaviours. We believe that a good start point is developing standards to categorise and label IoT devices according to their level of security. This is because, the rest of the solutions can be then more effectively applied once there is a benchmark of what is understood as "secure" in IoT, and what it is not. When education fails, the application of coercive measures should serve as a valid mechanism to preserve cybersecurity, as it does in other spheres of common interest such as traffic laws, environmental, health, and public safety affairs.

REFERENCES

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., et al. (2017). Understanding the mirai botnet. In *USENIX Security Symposium*.

Asghari, H., van Eeten, M. J., and Bauer, J. M. (2015). Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy*, 13(5):16–23.

Bauer, J. M. and Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10-11):706–719.

Boddy, S. and Shattuck, J. (2018). Threat analysis report. the hunto for iot. the growth and evolution of thingbots ensures chaos. https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-the-growth-and-evolution-of-thingbots-ensures-chaos. Retrieved on: 2018-06-25.

Cerf, V. G. (2013). Revisiting the tragedy of the commons. *Communications of the acm*, 56(10):7–7.

Cole, R., Dodis, Y., and Roughgarden, T. (2006). Bottleneck links, variable demand, and the tragedy of the commons. In *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*, pages 668–677. Society for Industrial and Applied Mathematics.

Davidow, B. (2012). The tragedy of the internet commons. *The Atlantic*, 18.

den Hartog, F., Raschella, A., Bouhafs, F., Kempker, P., Boltjes, B., and Seyedebrahimi, M. (2017). A pathway to solving the wi-fi tragedy of the commons in apartment blocks. In *Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International*, pages 1–6. IEEE.

Fong, K., Hepler, K., Raghavan, R., and Rowland, P. (2018). Quantifying Consumer Costs of Insecure Internet of Things Devices. https://groups.ischool.berkeley.edu/riot/. Accessed on: 2018-05-30.

Gartner (2017). Gartner newsroom. http://www.gartner.com/newsroom/id/3598917/. Accessed on: 2017-07-30.

Greenwood, G. W. (2016). Altruistic punishment can help resolve tragedy of the commons social dilemmas. In *Computational Intelligence and Games (CIG), 2016 IEEE Conference on*, pages 1–7. IEEE.

Hardin, G. (1968). The tragedy of the commons. *Science*, 162(3859):1243–1248.

Herley, C. and Florêncio, D. (2009). A profitless endeavor: phishing as tragedy of the commons. In *Proceedings of the 2008 New Security Paradigms Workshop*, pages 59–70. ACM.

Iannela, R. (2017). Tragedy of the digital commons: Amplified zombies [opinion]. *IEEE Technology and Society Magazine*, 36(3):15–16.

IoT Security Foundation. Best practice user mark faq and terms of use. https://www.iotsecurityfoundation.org/best-practice-user-mark/. Accessed on: 2018-06-26.

Krebs, B. (2016a). Hacked Cameras, DVRs Powered Todays Massive Internet Outage. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage. Accessed on: 2017-02-22.

Krebs, B. (2016b). Senator Prods Federal Agencies on IoT Mess. https://krebsonsecurity.com/2016/10/senator-prods-federal-agencies-on-iot-mess/. Accessed on: 2018-05-30.

Lloyd, W. F. (1833). *Two Lectures on the Checks to Population: Delivered Before the University of Oxford, in Michaelmas Term 1832*. JH Parker.

Lutu, A. and Bagnulo, M. (2011). The tragedy of the internet routing commons. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5. IEEE.

Mansfield-Devine, S. (2016). Ddos goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare. *Network Security*, 2016(11):7–13.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q. (2010). A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10. IEEE.

Smith, M. (2017). The tragedy of the commons in the IoT ecosystem. https://computerworld.com.au/article/626059/tragedy-commons-iot-ecosystem/. Accessed on: 2018-05-30.

The European Parliament and the Council of the European Union (2016). General data protection regulation-gdpr. https://gdpr-info.eu/. Retrieved on: 2018-06-25.

Usman, S. H. (2013). A review of responsibilities of internet service providers toward their customer's network security. *Journal of Theoretical & Applied Information Technology*, 49(1).

World Economic Forum (2018). The global risks report 2018. http://weforum.org/docs/WEF$_{GRR}$18$_{Report.pdf}$/.