Alerting Consciences to Reduce Cybercrime

A Quasi-experimental Design Using Warning Banners

Asier Moneva [1,2] E. Rutger Leukfeldt [1,2] Wouter Klijnsoon [3]

[1] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR); [2] Center of Expertise Cyber Security, The Hague University of Applied Sciences; [3] Team High Tech Crime (THTC), Dutch National Police

Abstract

Objectives: Aiming to reduce distributed denial-of-service (DDoS) attacks by alerting the consciences of Internet users, this paper evaluates the effectiveness of four warning banners displayed as online ads (deterrent—control, social, informative, and reorienting) and the contents of their two linked landing pages. *Methods:* We implement a 4 x 2 quasi-experimental design on a self-selected sample of Internet users to measure the engagement generated by the ads and the pages. Engagement is measured on the ads as the ratio of clicks to impressions, and on the pages as percentage of page scrolled, average session duration, video interaction rate, and URLs click rate. *Results:* Social ads generate significantly more engagement than the rest with low to medium effect sizes. Data reveal no differences in engagement between both landing page designs. *Conclusions:* Social messages may be a better alternative for engaging with potential cyber offenders than the traditional deterrent messages.

Correspondence: Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan 1077, 1081 HV, Amsterdam, The Netherlands. *Email:* AMoneva@nscr.nl

---

This version of the article has been accepted for publication, after peer review (when applicable) but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: https://link.springer.com/article/10.1007/s11292-022-09504-2. Use of this Accepted Version is subject to the publisher's Accepted Manuscript terms of use https://www.springernature.com/gp/open-research/policies/acceptedmanuscript-terms.

1 Introduction

Would the chess grandmasters Garri K. Kaspárov and Anatoli E. Kárpov have played chess if they had been born in the 2000s? Given the undeniable appeal of chess, the answer would probably be yes. However, at present, where digital entertainment is so advanced, the question poses a reasonable doubt. There are now established video game competitions in which individuals challenge their skills against each other. These competitions are followed by millions and are considered a proper sport by many, to the point that some have portrayed electronic sports or *e-sports* as the chess of the 21st century (Pluss et al. 2019). E-sports are now more popular than ever and the gaming industry generates enormous profits (e.g., Miu et al. 2020; Jenny et al. 2018), a trend that was accentuated during the COVID-19 pandemic (Amin, Griffiths, and Dsouza 2020). Unfortunately, we will never know whether Kaspárov and Kárpov would have become popular streamers, battling it out for the world championship in the game of the century. We do know, however, that today's youth have a clear preference for gaming.

The popularity of the gaming industry, however, has also made it a target for cybercrime. Empirical research shows that one of the cyber-dependent crimes that most affects this industry are distributed denial of service (DDoS) attacks (Brunt, Pandey, and McCoy 2017; Collier et al. 2019; Miu et al. 2020; Noroozian et al. 2016). DDoS attacks are aimed at congesting online services with massive amounts of Internet traffic, so that they become unavailable to their legitimate users (Lau et al. 2000). Disabling online services can cause organizations huge economic losses both directly, due to an inability to provide the service, and indirectly, due to a loss of confidence in the provider. In an industry like gaming with an estimated revenue in the billions (Miu et al. 2020), these losses can amount to millions. Data from 2014 and 2015 revealed that 42% of 132 domains victims of DDoS attacks were related to the gaming industry through video games such as Minecraft, Counter-Strike, and Runescape (Noroozian et al. 2016). Similarly, a recent technical report shows that 31.7% of the DDoS attacks recorded in the third quarter of 2020 targeted companies in the online gaming sector such as Nitrado, Gameservers.com, and Blizzard Entertainment, among others (Miu et al. 2020). The real-time nature of online gaming makes stable connections essential not only for an enjoyable experience for players, but also for the integrity of the competition. This makes e-sports especially vulnerable to DDoS attacks, which can take down the servers hosting an e-sports competition, the communication channels used by the players, the computers of the streamers broadcasting a live event, or those of the players themselves.

It might seem that carrying out a DDoS attack is only within the reach of a few, both in terms of infrastructure and knowledge, but the reality is different. As would be the case in any healthy market, the growing demand for this 'product' has led to its offering as a service online. For about "$15 for a monthly subscription, up to $1,980 for a lifetime subscription" (Hyslip and Holt 2019, 1612), 'customers' can rent a bot-infected network of computers known as a *botnet* to coordinate a DDoS attack, purchase software to build their own botnet, or even buy the bots separately (Hyslip 2020; Miu et al. 2020). Other services even offer free attacks (Hyslip and Holt 2019). This requires the user to be able to operate and maintain the software. But now not even that is necessary. Through for example PayPal or cryptocurrencies, customers can purchase these services directly from third parties, without having to configure and maintain them, through so-called booters and stressers (Hutchings and Clayton 2016; Hyslip and Holt 2019). Through single purchases or monthly subscriptions, customers are able to *boot* users from a network or *stress* the capacity of specific servers to handle loads of Internet traffic; the equivalent to kicking players from online games and overloading gaming servers. DDoS services are sometimes advertised on the dark web in criminal forums, hacker forums and websites, but as is the case in any business, being easily found is good for financial gain (Hyslip 2020; Hutchings and Clayton 2016). In most cases, all it takes to access this illicit market is to query a search engine on the clear web with the right keywords as some DDoS suppliers even advertise on Google.

Internet users intrigued by DDoS attacks can find clues in online communities such as Telegram or Discord that focus on hacking or gaming (see Collier et al. 2021). These users may also seek information through search engines such as Google or browse how-to tutorials through video platforms such as YouTube. This first contact can sometimes become a pathway into cybercrime. One of the problems is that many of the users who start experimenting with DDoS attacks do not know that what they are doing is illegal, nor do the people around them. If students throw a brick through their school window, they will be corrected by teachers, parents and peers; however, if they saturate the servers of their school with DDoS attacks, the

response will not be so obvious. So neither the behavior would be corrected at an early stage nor the threat of punishment would be effective. Over the years, this pathway can lead to a cybercriminal career (Ruiter and Bernaards 2013). Cybercriminals then professionalize and their illicit behavior becomes chronic. In these cases, it is often too late for educational prevention and intervention strategies to be effective. When young people go down this path, society not only suffers the consequences of cybercrime but in some cases also wastes IT talents that could otherwise be put at the service of cybersecurity (Schiks, van 't Hoff-de Goede, and Leukfeldt 2021).

Aware of the DDoS problem, and of how Internet users first engage in foul play, the National Crime Agency (NCA) of the United Kingdom launched a Google Ads campaign to deter and divert juvenile cyber offenders from carrying out DDoS attacks. From December 2017 to June 2018, the NCA used Google's services to display messages such as "DDoS is an offence in the UK" and "DDoS is illegal" whenever a user searched for a series of terms related to DDoS attacks. The effect of this campaign on the volume of attacks was incidentally captured in a study that collected DDoS data in several countries using honeypots. The study revealed that the growing trend of DDoS attacks flattened out in the United Kingdom over the course of the campaign, while no such change was observed in comparable countries such as France, Germany, the Netherlands, and the United States (Collier et al. 2019). Although this evidence is promising, further replication of the study is needed to reach solid conclusions.

Furthermore, although Collier and colleagues (2019) examine the effect of the Google Ads campaign on the DDoS trend, no study has evaluated whether the message of the ads—or the content of their landing pages—was the most appropriate to alert the consciences of juveniles with the potential to become cyber offenders. In this regard, a recent qualitative study suggests that the design of online ads to prevent consumption of child sexual exploitation material may be key to improving their effectiveness (Henry 2020). So it is possible that the design of the ads and the landing pages (e.g., the text they contain, the tone of the message) affects their ability to generate more engagement among potential DDoS-ers. And that this, in turn, impacts on the effectiveness of the campaign to reduce DDoS attacks. To fill this gap, the present study aims to determine what is the best combination of ads and landing pages to alert consciences of Internet users interested in DDoS attacks. A form of advertising that fits into the broader category of warning banners.

2 Warning Banners for Situational Cybercrime Prevention

Unlike other preventive strategies that attempt to reverse the root causes of crime, situational crime prevention focuses on tackling the immediate causes of crime (Clarke 1980). Situational crime prevention assumes three things: crime is the result of the interaction between criminal motivation and a situation, offenders can decide whether to commit a crime, and opportunity plays an essential role in crime perpetration (Clarke 2017). Based on these assumptions, situational crime prevention articulates 25 techniques to reduce crime that operate through five mechanisms: increasing the effort to commit crime, increasing the risk of being detected when committing crime, reducing the rewards of crime, reducing provocations to potential offenders, and removing excuses for non compliance with the norm (Cornish and Clarke 2003; Clarke and Eck 2003). Through these mechanisms, situational crime prevention has proven its usefulness in multiple contexts (e.g., Clarke 1997; Felson and Eckert 2019), which has led criminologists to extend its application to online environments.

One of the first adaptations of the situational crime prevention framework to cyberspace was aimed at reducing e-commerce crime (Newman and Clarke 2003). Among its recommendations was to alert consciences and control disinhibitors by referring to specific criminal acts through campaigns and posters, such as "copying software is punishable by prison" and "hackers cause serious personal and financial damage" (p. 134). These campaigns and posters became what current empirical research terms warning messages or *warning banners*: digital texts that are automatically displayed to potential cyber offenders before they commit a cybercrime (see Brewer et al. 2019). Warning banners represent a way of curbing certain behaviors by giving potential cyber offenders *an informed choice*. These warnings have been mainly used to deter hackers from trespassing on systems (e.g., Maimon et al. 2014; Testa et al. 2017), although they have also recently been used to reduce the number of visitors to barely legal pornography sites (Prichard et al. 2021), or to divert Internet

users from carrying out DDoS attacks (see Collier et al. 2019). To measure the effectiveness of banners, many studies collect data from potential cyber offenders through honeypots.

In a broad sense, honeypots are computer resources (e.g., computer networks, accounts, ads) designed to attract Internet users to interact with them (Prichard et al. 2021; Spitzner 2003; Vetterl 2020). Cybercrime researchers use honeypots to simulate online targets in controlled environments as to collect objective measures of cybercriminal behavior. By having control over the honeypot, researchers can assign groups of users to different stimuli and thus evaluate their effect. For example, researchers can evaluate the effect of different warning banners displaying unique messages on system trespassing behavior. Now, warning banners have been designed to take advantage of two situational crime prevention mechanisms: increasing the perceived risks, and removing excuses. To increase perceived risks, warning banners often incorporate deterring messages that point to the presence of surveillance (e.g., user activity is being monitored in this system) or invoke the threat of sanction (e.g., unauthorized trespassing is subject to legal penalty); to remove excuses, warning banners alert consciences by informing about the illicit of an action (e.g., DDoS attacks are illegal) or the harm that a specific behavior may cause (e.g., cybercrime can inflict serious damage).

In general, honeypot experiments on warning banners—most of them aimed at diverting hackers—have yielded mixed results. For example, research has shown that while warning banners do not reduce the probability of an initial trespassing incident (Maimon et al. 2014; Vetterl 2020), some messages can reduce the number of simultaneous sessions initiated by hackers in trespassed systems (Fisher, Maimon, and Berenblum 2021). Experimental research has also shown that, except in one case with a very small effect size (Fisher, Maimon, and Berenblum 2021), deterrent warning banners have no effect on repeat intrusions (Maimon et al. 2014; Vetterl 2020; Wilson et al. 2015). On a positive note, one of these experiments and its replicate have shown that these banners can significantly reduce the duration of trespassing incidents (Maimon et al. 2014; Stockman, Heile, and Rein 2015). However, this finding has also been contested recently (Vetterl 2020). Furthermore, research has shown mixed results regarding the effect of warning banners on the number and type of commands entered inside the trespassed system: either these messages do not reduce commands at all (Jones, Maimon, and Ren 2017; Howell et al. 2017), only some types of messages do (Jones, Maimon, and Ren 2017; Fisher, Maimon, and Berenblum 2021), they reduce only certain types of commands (Testa et al. 2017), or they only have a reduction effect on the longest incidents (Wilson et al. 2015). Finally, when deterring warning banners have been directed at a different target group, visitors to barely legal pornography sites, results have shown a significant reduction in the number of visits (Prichard et al. 2021).

Experimental research using honeypots to test the effect of warning banners has not been without criticism though. The most important criticism is that these honeypots would not be collecting data on the effect of warning banners on potential cyber offenders, but on bots (Vetterl 2020). Therefore, any effect resulting from warning banners would be unreliable, since—for the time being—neither the bots have a conscience to alert nor are they deterred by the threat of sanction. As new generations of honeypots improve in their ability to distinguish human from bot activity, there are alternatives for measuring the effect of warning banners on potential cyber offenders.

Google Ads, an accessible and cost-effective platform, claims to be able to detect bot activity and remove it from the data log (Google 2021b)[1]. Considering a mean cost of €2 per click on an ad, and 50 clicks per day, one can maintain a targeted advertising campaign for four weeks with €2800 as part of an *influence policing* strategy (see Collier et al. 2021 for an explanation of this concept). In this way, clear and brief messages targeted to a specific audience can be broadly delivered, backed up by an authoritative source. The police may be one such source of authority, but in the case of DDoS attacks against the gaming industry, so may a prominent gaming company. Using the name or logo of such authorities can increase the credibility of warning messages and thus enhance their preventive ability (Prichard et al. 2021; Wogalter and Mayhorn 2008). In addition, Google provides additional socio-demographic information on users interacting with warning banners, a variable that was not previously reported. In the present study, we opted for Google Ads.

[1]Although the empirical data do not show any anomalies that we cannot explain, we do not have access to empirical data on the effectiveness of Google's anti-bot algorithms to corroborate such claims.

3 The Present Study

Building upon the 2018-2019 Google Ads campaign launched by the NCA in the United Kingdom, the present study implements its own campaign to determine what is the most effective ad-based communication strategy to reach Internet users interested in targeting the gaming industry with DDoS attacks. To inform the basic strategic objectives of deterrence and diversion of the original campaign, we examine: what kind of users interact with the ads, what keywords generate the most engagement, which type of ad is more engaging, when do users interact with the ads, how many users did actually navigate the landing pages, and on which landing page did users interact most with the content. To do so, this study deploys a set of four Google Ads and two linked landing pages in a quasi-experimental 4 x 2 factorial design. The stimuli rely on two sources of authority: the Dutch National Police or *Nationale Politie*, and ESL Benelux—a leading company in the gaming industry. The purpose of the ads and landing pages is to eliminate users' excuses for non-compliance with the norm by offering them an informed choice; this is, alerting their conscience in line with the 23rd measure of Situational Crime Prevention (Cornish and Clarke 2003). We then compare the performance of the ads and the landing pages in terms of engagement to determine which combination best serves this purpose.

4 Research Design

The research design begins with the selection of a series of keywords that mimic those used by users interested in carrying out DDoS attacks. When users search for any of these keywords in Google, the search results return one of the four ads—the first experimental condition. Since Google Ads does not support the random display of ads, we opt for the next best strategy: to rotate the ads indefinitely around searches. This option disables the automatic optimization of the ads performance and assigns users to one of the four initial experimental conditions more evenly. It is not possible for users to control which ad will be shown next with their search. This set-up allows us to approach randomization and determine which ad generates the highest engagement. Now, each ad is duplicated and each replica is linked to one of the two landing pages. By clicking on the ads, users land on one of the pages—the second experimental condition. The assignment to this second experimental condition is again not random, but the rotation of the ads makes it even between the two groups. The landing pages, hosted in the Netherlands, are prepared to collect a series of measures about the online behavior of their visitors. This allows us to compare which page design generates the most engagement among users. Collectively, the research design allows us to determine which is the best combination of ad and page to engage potential cyber offenders who want to target the gaming industry with DDoS attacks (see Figure 1)[2]

4.1 Users

Participants in our experiment are Internet users who self-select themselves when searching for information related to DDoS attacks in the Google search engine. Google then collects information from users based on their account information, including their age and gender. When these are not provided by users themselves, Google tries to infer this information based on their activity or by extracting information from their online profiles. When the demographic information of users cannot be identified, Google includes them in the category *unknown*. Data on gender distinguishes the categories *male*, *female*, and *unknown*. And data on age covers the intervals *18-24*, *25-34*, *35-44*, *45-54*, *55-64*, *65+*, and *unknown*. Due to Google's policy, minors are included in the category unknown. Samples of gamers in previous research report an average age of early twenties (Dieris-Hirche et al. 2020; Cole and Griffiths 2007). Meanwhile, cybercrime research suggests that the peak of offending is reached in youth and for some cybercrime types in adolescence (Brunton-Smith and

[2]All data manipulation and analyses were carried out in R version 4.1.2 (R Core Team 2022) and RStudio version 1.4.1 (RStudio Team 2022) using the following R packages: Tidiverse version 1.3.1 (Wickham et al. 2019), here version 1.0.1 (Müller 2020), and readxl version 1.3.1 (Wickham and Bryan 2019). Tables and Figures were created using knitr version 1.36 (Xie 2015), kableExtra version 1.3.4 (Zhu 2021), ggsignif version 0.6.3 (Ahlmann-Eltze and Patil 2021), and patchwork version 1.1.1 (Pedersen 2020). The manuscript was written in Rmarkdown version 2.11 (Xie, Allaire, and Grolemund 2018).

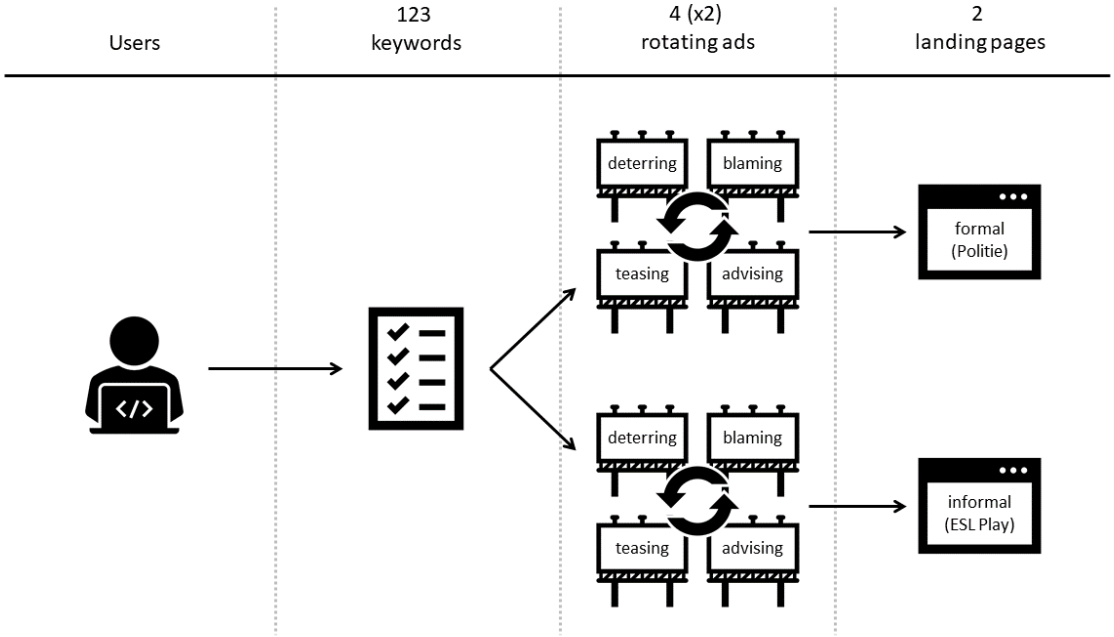


Figure 1: Research design

McCarthy 2016; Holt 2019). To reach this target group, our ad campaign only targets young people under the age of 35 and users included in the category unknown[3].

4.2 Keywords

In an attempt to capture the interests of these users, members of the Dutch National Police, together with professionals from the gaming industry, online ads experts, and academic criminologists compiled a list of 123 keywords related to DDoS attacks and video games. This list includes keywords such as: *how to DDoS*, *IP stresser*, *free stresser*, *PS4 booter*, *DDoS Twitch*, and *DDoS Linux* (see Appendix A for the full list of keywords). Other parties may want to use the same keywords to advertise their services, so the same keyword can be linked to several ads. This means that, to position their ad as well as possible (i.e., first page, top row), interested parties must compete. Several factors influence this competition: the relationship between the user's search and the keyword; the quality of the ad, which in turn is based on multiple factors, such as the likelihood that users will click on the ad and their experience once they visit the landing page; and the price that each competitor has paid to use the keyword. The price paid for each keyword—its cost per click in euro (€)—is determined by an auction where each party bids for its interests. Therefore, when there is high competition for a keyword, its price rises. It is important to understand how these factors combine to ensure a good positioning of the ads, since a bad management can cause the ads not to be shown at all.

To allow flexible audience targeting with ads, Google offers three types of keyword matching: *broad match*, which is the least restrictive and hits searches related to the keywords but different; *phrase match*, which is moderately restrictive and hits searches that include the meaning of the keywords; and *exact match*, which is the most restrictive and only hits searches with the same meaning as the keywords. For example, for the keyword *how to DDoS*, a broad match would be *how to make your own DDoS booter*, a phrase match would be *how to DDoS a game server*, and an exact match would be *how to DDoS*. Note that phrase match and

[3]As is the case with online surveys, note that nothing prevents users from editing their profiles to provide false information. While we believe that most users are honest, we recommend that this information is interpreted with caution

Table 1: Content of the ads by control and experimental groups

Group	Tone	Headline 1	Headline 2	Description
control	deterrent	A DDoS attack is illegal	Gamechangers	Carrying out a DDoS is illegal in the Netherlands under the Criminal Code
experimental 1	social	DDoS ruins it for everyone	Gamechangers	So you want your friends to be unable to play games because you play a prank?
experimental 2	informative	Do you want to DDoS a game?	Gamechangers	Learn more about DDoS attacks and their impact on gaming
experimental 3	reorienting	Play fair; losers do DDoS	Gamechangers	Win fairly in an e-sports competition by training your gaming skills

exact match also support close variants of the keywords. In our example, a close variant of an exact match would hit *how can I ddos someone*. Since we were interested in reaching the users most at risk of carrying out a cyber-attack, most of the keywords were configured to hit exact or phrase matches. Users whose searches match our keywords in any way would see one of our ads.

4.3 The ads

The first experimental condition users face is exposure to four online ads. Each ad displays a unique text, which varies in tone, but has similar length and appearance. For their design we recycled the deterring ad used by the NCA in their campaign, which was then translated into Dutch and used as a control. It is common in criminology experiments that the control group also receives some kind of stimulus (Weisburd, Petrosino, and Fronius 2014), which in this case represents the traditional way of presenting a *deterrent* message by the police. The other three ads constitute the experimental conditions showing alternative forms of communication: *social*, *informative*, and *reorienting*. Table 1 shows the configuration of the ads (for the original ads, in Dutch, see Appendix A). Each tone is articulated as follows:

- Deterrent: Uses the illegality of the conduct to invoke the threat of a legal sanction.
- Social: Uses social consequences of behavior to invoke potential negative reinforcement from peers.
- Informative: Uses a click-bait to provide additional information about DDoS attacks.
- Reorienting: Uses gaming jargon to suggest alternative pro-social behavior.

A Google Ads account was set up to quantify the engagement generated by the ads in each group through the following three measures:

- Impressions: the number of times the ad is shown.
- Clicks: the number of times a user clicks on an ad.
- Engagement: the ratio of clicks to impressions.

Since ads are not always displayed in the top row of the search results (78.5% of the time in our case), better positioned ads might be benefiting from higher user engagement. This would bias comparisons. For this reason, we only compared metrics between those ads that were displayed in the top row of search results. Users who clicked on the ads were then redirected to a landing page.

4.4 The landing pages

The second experimental condition consists of exposure to one of two landing page designs: a formal one, endorsed by the Dutch National Police, and an informal one, endorsed by ESL Play—the world's largest independent e-sports league. The landing pages are simple websites hosted on a neutral domain called *Gamechangers*[4]. Their content is structured in four sections that provide information related to DDoS attacks. The first section explains what a DDoS attack is and includes a short explanatory video of about one minute featuring a uniformed police officer or the chief executive officer of ESL Benelux. The second section explains what the consequences of a DDoS attack are and includes three URLs that lead to additional content. The third section, accompanied by an image, explains where the legal limits of DDoS are and includes three more URLs. Finally, the fourth section shows some alternatives for visitors to take advantage of their IT talent and includes a further three URLs. In short, each landing page contains text, a video, an image, and nine URLs, and is long enough that users have to scroll down a little to see all the content (Appendix B shows the landing pages). However, all this information can only be meaningful if users interact with it.

To measure user interaction in the pages, a Google Analytics account was set up. Note that when linking a Google Ads account with a Google analytics account, there can be several reasons for data discrepancies, like page redirects, and server latency issues, among others (Google 2021a). We identified a 7.3% discrepancy between the number of clicks on our ads and the number of new users who visited our landing pages. Considering the high bounce rate we observed (i.e., the ratio of users who landed on our pages and left immediately thereafter), this difference may represent users who click on the ads but leave the landing page before the tracking code executes.

Since the landing pages are in the open, it is possible for a visitor—although very unlikely—to reach them directly by typing their URL, thus bypassing the ads. It is also possible for the same user to access landing pages several times through recurring keyword searches. This would bias the metrics. To ensure that only relevant user traffic is analyzed, a custom data segment was created in Google Analytics to filter out users who had reached the landing pages by other means than ads and had opened more than one web session (20.6%). User sessions are interrupted after 30 minutes of inactivity, at midnight, or when leaving the landing page and accessing it again by reaching the ads through a different set of keywords. With this filter in place, 99.6% of the remaining users were new visitors of the landing pages, so we expect the impact of returning users on the data to be negligible.

To determine which landing page generates the most engagement among visitors, snippets of HTML tracking code were added to the source code of the website to capture user interactions with certain elements called events. These events are:

- Scrolling depth: percentage of landing page scrolled, with breaks at 25%, 50%, and 75%.
- Video interactions: number of times a video was started, paused, sought or advanced to a specific point, and completed.
- URL clicks: number of times each of the nine URLs was clicked.

Sometimes, particularly active users can inflate the number of times these events are triggered. To avoid inflated counts and to be able to make a more meaningful comparison of users' behavior in the landing pages, we measured *unique events* instead of total events. That is, we measured the number of times these events were triggered at least once per session. This indicates whether or not the event generated engagement regardless of how many times it did so.

[4]The Gamechangers platform was created by the Dutch National Police in April 2020 to offer youth interested in IT appropriate challenges during the onset of the COVID-19 pandemic. The platform partners with private companies and is not necessarily associated with the police.

4.5 Pilot study

In order to assess the validity of the proposed quasi-experimental design, the online ads campaign was launched along with the landing pages on 8 January 2021 and their performance was monitored until 22 January 2021, for a total of 15 days. After verifying that the ads rotated indefinitely but unevenly among Google users and that both landing pages were receiving a similar amount of visitors, the pilot was deemed successful and the final experiment was implemented.

4.6 The campaign

The final campaign ran for 14 weeks, from 23 January 2021 to 30 April 2021. During this period, the ads generated a total of 71475 impressions and 4457 clicks, which yield a mean engagement ratio of 6.2% (Figure 2). As can be observed, impressions and clicks are positively, strongly, and significantly correlated ($r(96) = 0.805$, $p < 0.001$). The large spike recorded on March 22, caused by a high volume of DDoS-related searches, coincides with a large DDoS attack in the Netherlands recorded by the Dutch National Police.

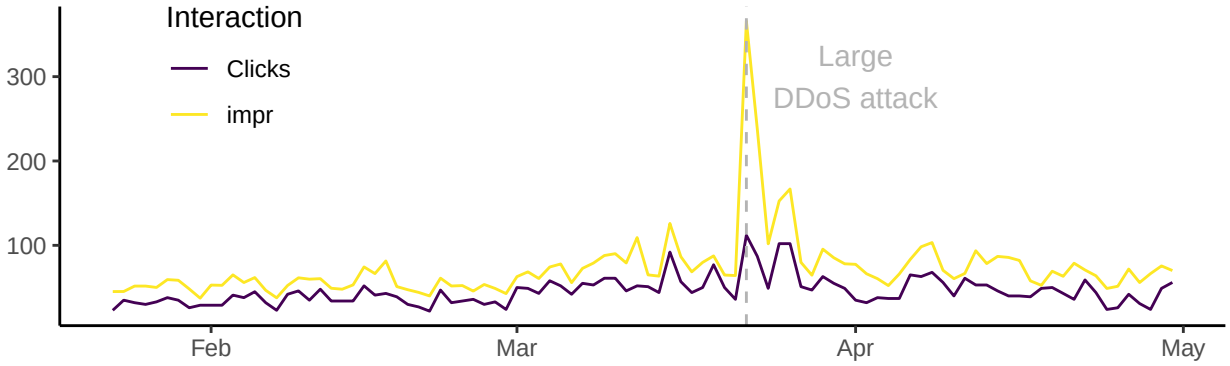


Figure 2: Google Ads campaign duration and interaction metrics

5 Results

For the ads to be effective in preventing DDoS attacks against the gaming industry, they must reach the right target group. Based on the demographics of the gaming community and early career cybercriminals, we assumed those engaging with the ads would be mostly young males. Figure 3 indicates that the users who search for the keywords that trigger the ads (i.e., impressions) and those who click on them (i.e., clicks) are almost entirely male. Out of the 71475 impressions, 43.3% were caused by males and 6% by females; out of the 4457 clicks, 58% were caused by males and 5.7% by females. The majority of users fall within the *18-24* and the *unknown* age group, which supports the idea that it is the youngest users who are most engaged with the ads. It should be noted that Google classifies underage users as unknown, along with users who do not provide sociodemographic data.

We also examined what keywords were entered by users who searched for DDoS-attack related terms. For an ad campaign to be economically sustainable, it is important to identify not only the keywords that generated most engagement, but also those that did so at the lowest cost per click in € (i.e., the most efficient keywords). For those keywords that generated at least 25 clicks ($n = 34$), Figure 4 shows, in four quadrants, the relationship between the engagement generated, in the vertical axis, and the mean cost per click, in the horizontal axis. Quadrants are delimited by the average medians of the two variables displayed. As a result, the upper left-hand quadrant shows the most efficient keywords, while the bottom right-hand

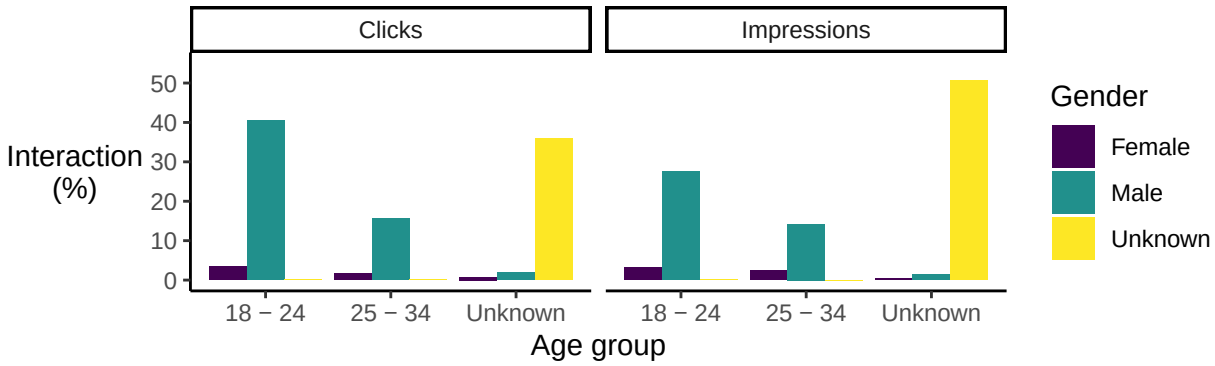


Figure 3: User target group

Table 2: Ad performance

	Impressions		Clicks	
Ad headline	n	%	n	%
DDoS ruins it for everyone	19678	35.1	1833	42.2
A DDoS attack is illegal	15484	27.6	1173	27.0
Do you want to DDoS a game?	12527	22.3	878	20.2
Play fair; losers do DDoS	8414	15.0	456	10.5

quadrant shows the least efficient ones. The colors display the type of match that corresponds to each keyword.

In addition, we compared the performance of the English and Dutch keywords to see if there were any differences. Although there were only 4 records in Dutch in our final list of 34, when we compared the weighted means of engagement ratio and cost per click generated by the keywords in both languages, we observed that the Dutch keywords generated higher engagement at a slightly lower cost. The engagement ratio for the Dutch keywords was 11.6 at a cost of 2.1, while for the English ones it was 8.2 at a cost of 2.2.

Users searching for these keywords were shown one of the ads. To compare ad performance and identify the most engaging, we only used data collected when the ads appeared among the top results. This corresponds to 78.5% of total impressions (56103) and 97.4% of total clicks (4340). The interaction generated by the ads, measured as impressions and clicks, was compared using descriptive statistics in Table 2. To determine whether the differences in engagement observed between the experimental ads and the control one were statistically significant, we conducted Chi-square tests of independence. Then we also calculated the log odds ratio to determine the size of the effect.

Results in Figure 5 show that the social ad generates significantly more engagement than the deterrent (i.e., control) [X^2 (1, N = 38168) 28.105, $p < 0.001$; *log OR* = 0.207]; that there is no difference between the informative and deterrent ads [X^2 (1, N = 30062) 2.755, $p = 0.097$; *log OR* = -0.078]; and that the reorienting ad generates significantly less engagement among users than the deterrent one [X^2 (1, N = 25527) 34.699, $p < 0.001$; *log OR* = -0.335]. Note that, in all cases, the size of the effect is small (J. Cohen 1988). Further analyses show that the differences between the informative and the reorienting ads are also significant, with a small effect size [X^2 (1, N = 22275) 18.57, $p < 0.001$; *log OR* = -0.257]. Finally, the differences between social and reorienting are indeed significant and with a medium effect size [X^2 (1, N = 30381) 102.523, $p <$ 0.001; *log OR* = -0.542].

Further descriptive analyses of the temporal dimension of user interaction with the ads reveal behavioral patterns. Figure **??** shows the mean user interaction with the ads per (A) day of the week, (B) hour of the

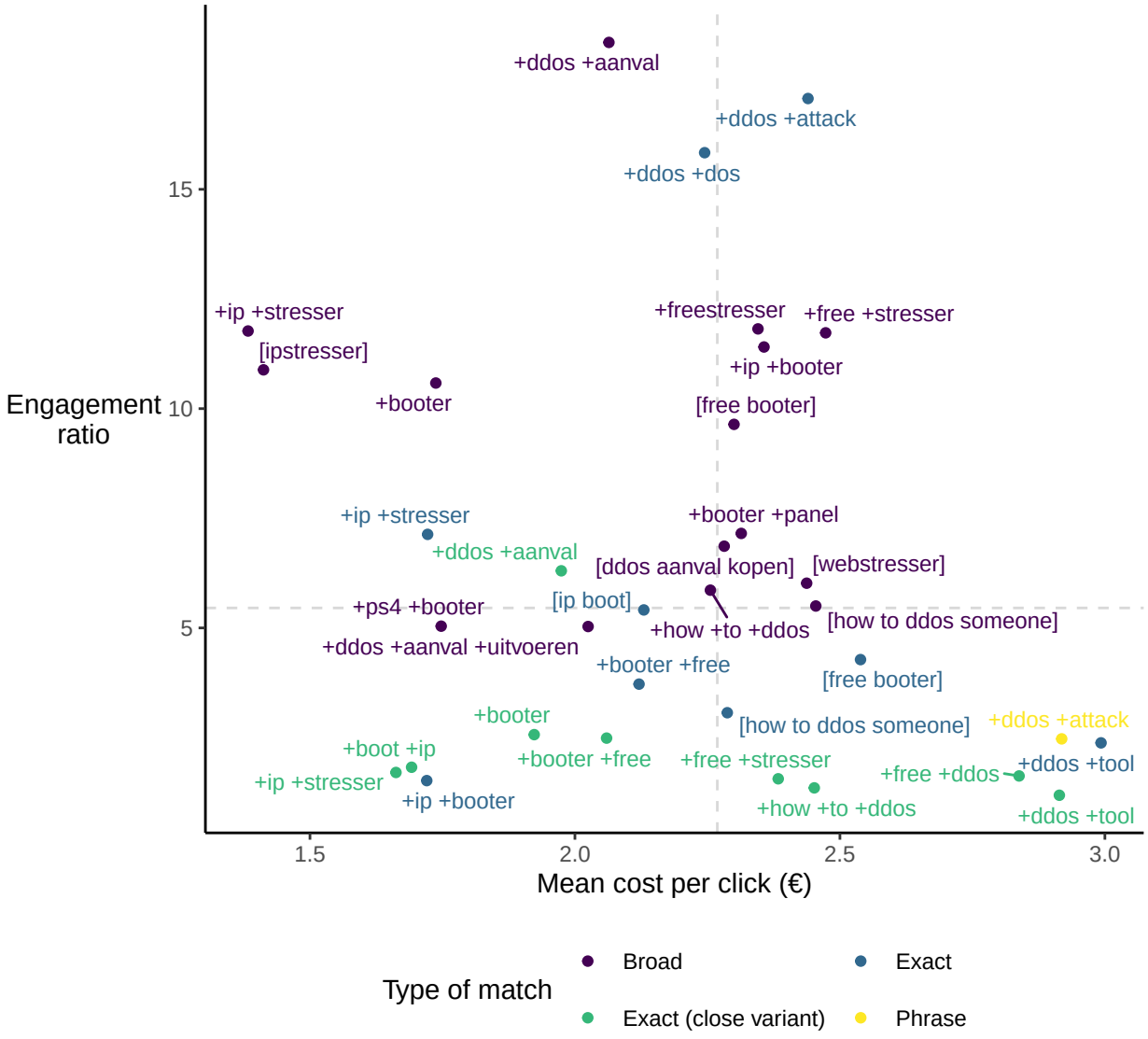


Figure 4: Keyword performance in terms of engagement generated versus mean cost per click in euro (€)

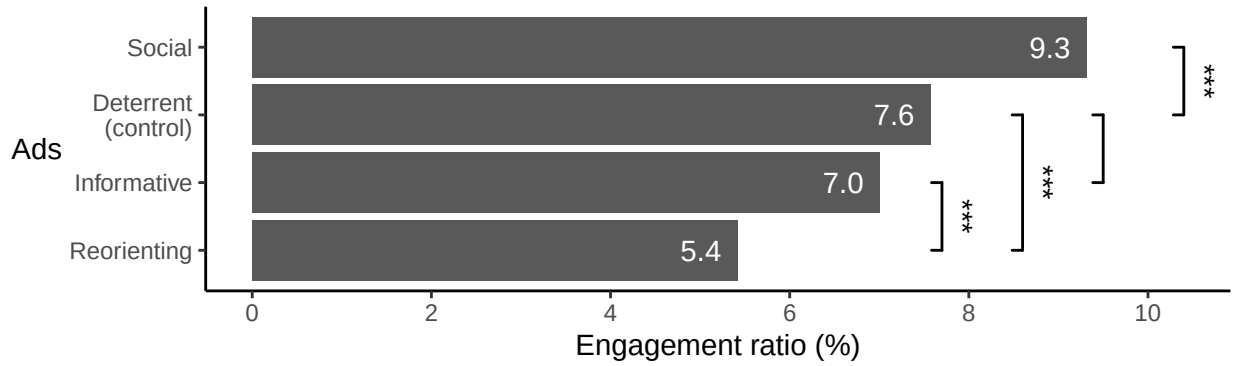


Figure 5: Differences in ad perfomance

Table 3: New users behaviour by landing page

	Users			
Landing page	n	%	Mean session duration (s)	Mean bounce rate (%)
Formal	1538	48.3	17.2	84.9
Informal	1645	51.7	17.9	84.7

day, and (C) both dimensions together. Data shows that the engagement ratio varies little between days, increasing as the week progresses and finally peaking on Sundays (Figure **??** A). As for the time of day, while the highest number of impressions is reached in the afternoon, engagement peaks at late night, between 1 and 3 am (Figure **??** B). When breaking down the time patterns by hours of each day, the engagement ratio tends to be homogeneous during the day, but varies greatly during the night hours. In some time slots, due to small data counts, user interaction yields extreme engagement values (Figure **??** C) .To avoid misinterpretation, these figures have been removed and are now shown as empty cells.

Whatever the time of day, by clicking on the ads, users end up on a landing page. After removing returning users, our two landing pages registered a total of 3183 new visitors, about half of which landed on one or the other landing page. Both user groups display an almost identical behavior (Table 3). Of the 1538 (48.3%) users who landed on the informal page, 84.9% bounced immediately and the remaining 15.1% spent an average of 17.2 seconds browsing it. Very similar data can be gleaned from the formal page. Of the 1645 (51.7%) users who landed there, 84.7% bounced and the remaining 15.3% spent an average of 17.9 seconds on the page.

Events allow to further examine the number of interactions generated on each landing page. Visual examination reveals no differences between total interactions in both landing pages (Figure **??** A). When further breaking down the data, it seems that users scroll down to the bottom of the informal page to the same extent in both pages (Figure **??** B). And we observe no differences in the video interactions either (Figure **??** C). Finally, the inconsistent distribution of interactions with URLs, also suggests that our two landing page designs do not have a distinct effect on user behavior (Figure **??** D).

6 Discussion

Building on the previous work by the NCA and Collier and colleagues(2019), this study implemented a quasi-experiment to determine what is the most effective ad-based communication strategy in engaging young Internet users interested in DDoS attacks. Using Google Ads, we deployed a far-reaching communication

campaign in the Netherlands consisting of four rotating online ads and two linked landing pages containing different messages. The campaign generated 71475 impressions and 4457 clicks within 14 weeks. Throughout this time, impressions and clicks remained strongly correlated, even when a large interaction spike was recorded. This spike overlapped with a large DDoS attack recorded by the Dutch National Police, suggesting that the impressions generated by online ads linked to DDoS-related keywords could be used as a proxy measure of actual DDoS attacks. In addition, Google Analytics was used to collect personal and behavioral information about the users who clicked on the ads and visited the landing pages. Google's tools allowed us to export multiple data sets to evaluate the performance of our campaign in detail. There is hardly any other way to reach so many people about to find something illegal on the Internet, inform them of the illegality and impact of a conduct—of some legal alternatives as well—and collect data on their online behavior in such a short time and with limited resources.

Google Ads and Google Analytics are tools designed to rigorously measure the objective behavior of real users, not bots. Unlike other studies using honeypot networks, which have been criticized for not discriminating between human and bot behavior (see Vetterl 2020), this study relies on Google's technology to filter out unwanted traffic, such as bots and other automated sources (Google 2021b). But these tools also have limitations. Perhaps the most important issue for research purposes is the lack of transparency with regard to the anti-bot algorithms and the randomization method for assigning users to different ads. Instead, there is the option to "rotate ads indefinitely," which distributes users more evenly between ads than other alternatives, but less so than randomization would—a setup that defines this quasi-experiment. From a methodological point of view, we believe that Google's tools have great potential to facilitate social research on online phenomena such as cyber offending.

Compared to other online advertising campaigns, the engagement—or click through rate—generated by our ads was high. In a criminological context, fake banners to access barely legal pornography sites generated an engagement of 1.4% (Prichard et al. 2021). In other contexts, Google Ads' standardised metrics allow to compare results. For example, a study on abortion that used Google Ads combined with an informative landing page to recruit participants had an engagement ratio of 1.7% (Upadhyay et al. 2020). Another study that tested how different elements of Google Ads design affected click through rate found that the best designs yielded a maximum engagement of 7.6% (Atkinson, Driesener, and Corkindale 2014). The worst performing of our ads generated an engagement of 5.4% (reorienting), while the best one generated an engagement of 9.3% (social). In the absence of synthesis research to facilitate comparison, these results suggest that our ad design based on clear and short messages is quite effective in engaging with our target audience. Quantitative analyses of the engagement generated by the ads indicated that the best tone to attract the attention of potential DDoS-ers is the social, followed by the deterrent and informative, and last by the reorienting one. While the percentage differences between the 9.3% engagement generated by the social ad and the 7.6% generated by the deterrent ad may not seem important, in an online ad campaign that reaches tens of thousands of users, this is a significant difference.

By deploying online ads as warning banners to divert potential cyber offenders from targeting the gaming industry, this study extends the application of situational crime prevention to cyberspace (Newman and Clarke 2003; Brewer et al. 2019). Like the original campaign by the NCA, ours was intended to cut off pathways into cybercrime for juveniles. Using warning banners, we seek to remove any excuses such users might have to carry out DDoS attacks by alerting their consciences at a critical time: when they are expressing interest in DDoS attacks or are even about to execute them. In the spirit of focused deterrence (Kennedy 2012), the warning banners and their linked landing pages serve the triple purpose of informing the most inexperienced and unaware users that DDoS attacks are illegal, showing the legal consequences of carrying them out, and presenting prosocial alternatives for developing IT skills. Contrary to police tradition, our warnings appeal not only to the sanction associated with the illegality of conduct (deterrent), but also to other factors such as peer influence (social), curiosity (informative), and fairness (reorienting). In a similar vein, our landing pages do not just deliver a message in a classic formal tone, but also offer an informal alternative for those interested in IT. The reasoning behind this design is that not all messages may alert the consciences of all offenders in the same way.

Banners seem like a promising strategy to reach potential or early-career offenders. As such, we do not expect banners to be effective in reducing all types of cybercrime, but rather entry-level ones such as DDoS

attacks, Remote Access Trojan (RAT) malware infections, basic hacks enabled by manuals and tutorials, and phishing kits. Cyber offenders who need hire DDoS-attacks are likely to be inexperienced and lack the skills and resources to manage their own infrastructure. Their attacks often target sectors such as gaming, gambling, and education (Miu et al. 2020; Hutchings and Clayton 2016). We therefore expect our banners—and similar campaigns—to be more effective in engaging this population and protecting these sectors than others such as critical infrastructures, government, businesses, IT, and finance. The latter are often targeted by more experienced and even organized cybercriminals who probably do not need to hire cybercrime-as-a-service because they already operate their own infrastructure. While we cannot rule out that these cybercriminals find our warnings on Google, we do not believe that either the ads or the landing pages will have a strong deterrent or diverting effect because they already know that their actions are illegal and have negative consequences, and they probably make a lot of money from them. Just as offenders introduce cybercrime keywords in search engines, victims search for help. Therefore, banners could also be useful to inform cybercrime victims of threats or the existence of help desks. For example, banners could warn victims about tech support scams and redirect them to legitimate channels. In this way, large technology companies could mitigate the impact of scams targeting their services. Future research analyzing search terms related to entry-level cybercrimes and victim support may reveal new insights into how to use banners to reduce cybercrime and help victims.

Differences in engagement with the ads could be explained in the light of the Social Learning Theory applied to cybercrime (Navarro and Marcum 2020). One of the propositions of this theory is that criminal behavior is conditioned by a series of reinforcements that people receive from their social interactions (Akers 2009). Online games are an increasingly important source of social ties and one of the digital contexts in which the audience for our ads is likely to interact. There, the group that would mainly reinforce the behavior of users would be their gaming peers. Research suggests that, like social ties, these *digital ties* could also play an important role in committing cybercrime (e.g., Weulen Kranenbarg, Ruiter, and Van Gelder 2021; Leukfeldt, Kleemans, and Stol 2017). It is possible that our social message triggers the idea of a negative reinforcement by gaming peers that engages the audience better than other ads, thus generating more interaction. This interpretation would suggest that, where the aim of a prevention or intervention strategy is to engage with people rather than deter them, relevant authorities (e.g., police, gaming industry, Internet service providers) could benefit from using a social tone to formulate their messages. A paradigm shift in the traditional use of deterrent messages by the police which could be especially useful in *influence policing* strategies targeted at potential cybercriminals who are unaware of the illegality of a conduct (see Collier et al. 2021) and *focused deterrence* strategies targeted at chronic cybercriminals who would be open to considering alternatives to crime. Both strategies are a good example of why it is important to adapt communication to the target audience.

Not only is it important to adapt the messages to the target audience, but also the keywords that trigger them. Keywords are the keys that unlock the entire communication campaign, so it is critical to choose the right ones. That is why researchers should involve practitioners in their selection. While researchers might have substantive knowledge of the problem, practitioners bring invaluable everyday experience in the field. The expertise provided by the police, the gaming industry, and online ads experts in this study was instrumental in compiling an efficient keyword list. Such a list should strike a balance between mainstream terms, which serve the function of delivering the message to a broad audience (primary prevention), and terms that reflect the criminal interest of the users who search for them, which serve the function of reaching the at-risk population (secondary prevention). Note that not all words generate the same engagement nor do they cost the same. Given possible budgetary constraints, it is essential to develop sustainable campaigns, and efficiency is indeed key to this. To increase efficiency, our results suggest taking into account the languages spoken in the regions covered by the campaign. Non-English keywords are likely to cost less and generate the same or even higher engagement among native speakers than their English counterparts.

Considering the almost absolute penetration of the Internet in society, online ads campaigns represent a cost-effective alternative to traditional law enforcement strategies for reaching large numbers of people with warning banners. Google's tools offer new insight into the characteristics of such audience. According to Google's data, the vast majority of users who interacted with the ads were young males. This is consistent with studies examining the demographics of gamers (Dieris-Hirche et al. 2020; Cole and Griffiths 2007), and also with studies that situate the peak age of digital piracy just before the age of twenty (Brunton-Smith

and McCarthy 2016) and hacking below the age of thirty (Holt 2019). The large gender differences observed in this study also align with the gender gap described in the literature, which portrays hackers as mostly male (Steinmetz 2015; Steinmetz, Holt, and Holt 2020; Holt 2019). Our analyses shows a gender gap of 7.2:1 in impressions, and 10.1:1 in clicks in favor of males. While quantitative evidence on this gender gap is certainly relevant, these data is limited in this sense. Future qualitative research could provide deeper insights into who interacts with ads and why.

As for when, our results provide detailed information. Time patterns of interaction reveal that users perform more DDoS attacks-related searches on weekdays; however, the campaign generates higher engagement during the weekend, indicating that the proportion of users who are actually interested in the campaign is higher then. Interestingly, when looking at the daily time patterns, the peak of searches is reached in the afternoon, while the peak of engagement is reached during the night hours. Specifically, the average search pattern would peak on Monday afternoons, while the engagement pattern would peak in the early hours of Sunday (Saturday late night). A possible explanation for this—in line with routine activities (L. E. Cohen and Felson 1979)—could be that searches performed on weekdays are generic, with the objective of getting information on the subject in work or educational contexts, while searches on weekends are specific, with the objective of learning how to perform DDoS attacks or even hiring cybercrime services in a leisure context. So if impressions are a reflection of the general interests of users, and engagement is a reflection of the specific interest of a subset of users in DDoS attacks and the gaming industry, then the temporal distribution of engagement would help us understand the activity of DDoS-ers.

Findings also reveal that users do not engage with landing pages. Evidence of this are the high bouncing rate, the low average time spent on them, and the low rate of triggered events. The fact that users engage so little with landing pages suggests that their content should be brief and concise, without interactive elements such as videos or URLs taking on too much prominence. Low engagement may be due to landing page designs being too similar. Although this was purposely done to build comparable stimuli, future research should create—and compare—different designs. Low engagement could also mean that, after the first interaction with the ads, the text on the pages becomes less effective because it is repetitive. If user consciences were already alerted by the ads, the pages would not make them any more alert. In such a case, resources should be focused on designing better ads, leaving pages as mere containers for additional information.

The main challenge for future research should be to determine whether these types of online advertising campaigns actually reduce the volume of DDoS attacks. Past research found correlational evidence between the deployment of online ads campaigns and the volume of DDoS attacks recorded by honeypots (Collier et al. 2019). Future research should implement more robust research designs such as experiments and quasi-experiments to identify clear effects. Researchers should also explore the use of ads on other platforms such as YouTube that are being used by Internet users to learn how to do DDoS and other cybercrime. To collect DDoS attacks data, researchers can use a honeypot infrastructure such as the one owned by the Cambridge Cybercrime Centre, or look for alternative sources. It would be interesting to explore the possibilities offered by companies that regularly record DDoS data as part of their cyber security routine, such as Internet service providers. These companies in the private sector not only have the necessary infrastructure, but also the practitioner's expertise; they know the data and therefore also what are the most common types of attacks and targets. Collaborating with them may provide valuable insights.

7 References

Ahlmann-Eltze, Constantin, and Indrajeet Patil. 2021. "Ggsignif: R Package for Displaying Significance Brackets for 'Ggplot2'." https://doi.org/10.31234/osf.io/7awm6.

Akers, Ronald L. 2009. *Social Learning and Social Structure: A General Theory of Crime and Deviance*. New Brunswick, N.J: Transaction Publishers.

Amin, Kritika Premnath, Mark D. Griffiths, and Deena Dimple Dsouza. 2020. "Online Gaming During the COVID-19 Pandemic in India: Strategies for Work-Life Balance." *International Journal of Mental Health and Addiction*, July. https://doi.org/10.1007/s11469-020-00358-1.

Atkinson, Geoffrey, Carl Driesener, and David Corkindale. 2014. "Search Engine Advertisement Design Effects on Click-Through Rates." *Journal of Interactive Advertising* 14 (1): 24–30. https://doi.org/10.

1080/15252019.2014.890394.

Brewer, Russell, Melissa de Vel-Palumbo, Alice Hutchings, Thomas Holt, Andrew Goldsmith, and David Maimon. 2019. *Cybercrime Prevention: Theory and Applications*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1.

Brunt, Ryan, Prakhar Pandey, and Damon McCoy. 2017. "The 16th Annual Workshop on the Economics of Information Security (WEIS 2017)." In, 1–12. La Jolla, CA. http://www.infosecon.net/workshop/downloads/2017/pdf/Booted:_An_Analysis_of_a_Payment_Intervention_on_a_DDoS-for-Hire_Service.pdf.

Brunton-Smith, Ian, and Daniel J. McCarthy. 2016. "Explaining Young People's Involvement in Online Piracy: An Empirical Assessment Using the Offending Crime and Justice Survey in England and Wales." *Victims & Offenders* 11 (4): 509–33. https://doi.org/10.1080/15564886.2015.1121943.

Clarke, Ronald V. 1980. ""Situational" Crime Prevention: Theory and Practice." *The British Journal of Criminology* 20 (2): 136147. https://doi.org/10.1093/oxfordjournals.bjc.a047153.

———, ed. 1997. *Situational crime prevention: successful case studies*. 2nd ed. Guilderland, NY: Harrow; Heston.

———. 2017. "Situational Crime Prevention." In, edited by Richard Wortley and Michael Townsley, 2nd ed., 125. Crime Science Series 18. London, UK; New York, NY: Routledge, Taylor & Francis Group.

Clarke, Ronald V., and John E. Eck. 2003. *Become a Problem-Solving Crime Analyst: In 55 Small Steps*. London: Jill Dando Institute of Crime Science.

Cohen, Jacob. 1988. *Statistical Power Analysis for the Behavioral Sciences*. 2nd ed. Hillsdale, N.J: L. Erlbaum Associates.

Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44 (4): 588. https://doi.org/10.2307/2094589.

Cole, Helena, and Mark D. Griffiths. 2007. "Social Interactions in Massively Multiplayer Online Role-Playing Gamers." *CyberPsychology & Behavior* 10 (4): 575–83. https://doi.org/10.1089/cpb.2007.9988.

Collier, Ben, Daniel R. Thomas, Richard Clayton, and Alice Hutchings. 2019. "IMC '19: ACM Internet Measurement Conference." In, 50–64. Amsterdam Netherlands: ACM. https://doi.org/10.1145/3355369.3355592.

Collier, Ben, Daniel R. Thomas, Richard Clayton, Alice Hutchings, and Yi Ting Chua. 2021. "Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement Through a Market for Cybercrime Services." *Policing and Society*, February, 1–22. https://doi.org/10.1080/10439463.2021.1883608.

Cornish, Derek B., and Ronald V. Clarke. 2003. "Opportunities, precipitators and criminal decisions: A reply to Wortley´s critique of situational crime prevention." In, edited by Martha J. Smith and Derek B. Cornish, 4196. Crime prevention studies 16. New York, NY: Criminal Justice.

Dieris-Hirche, Jan, Magdalena Pape, Bert Theodor te Wildt, Aram Kehyayan, Maren Esch, Salam Aicha, Stephan Herpertz, and Laura Bottel. 2020. "Problematic Gaming Behavior and the Personality Traits of Video Gamers: A Cross-Sectional Survey." *Computers in Human Behavior* 106 (May): 106272. https://doi.org/10.1016/j.chb.2020.106272.

Felson, Marcus, and Mary Eckert. 2019. *Crime and Everyday Life: A Brief Introduction*. Sixth Edition. Los Angeles: SAGE Publications.

Fisher, Daren, David Maimon, and Tamar Berenblum. 2021. "Examining the Crime Prevention Claims of Crime Prevention Through Environmental Design on System-Trespassing Behaviors: A Randomized Experiment." *Security Journal*, January. https://doi.org/10.1057/s41284-020-00282-y.

Google. 2021a. "Data Discrepancies Between Google Ads and Analytics." https://support.google.com/analytics/answer/1034383.

———. 2021b. "Prevention of Invalid Clicks and Impressions." https://support.google.com/admanager/answer/1298900.

Henry, Claire. 2020. "Designing Effective Digital Advertisements to Prevent Online Consumption of Child Sexual Exploitation Material." *Journal of Child Sexual Abuse*, November, 1–23. https://doi.org/10.1080/10538712.2020.1841354.

Holt, Thomas J. 2019. "Computer Hacking and the Hacker Subculture." In, 118. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_31-1.

Howell, Christian J., David Maimon, John K. Cochran, Hattie M. Jones, and Ráchael A. Powers. 2017.

"System Trespasser Behavior After Exposure to Warning Messages at a Chinese Computer Network: An Examination," April. https://doi.org/10.5281/ZENODO.495772.

Hutchings, Alice, and Richard Clayton. 2016. "Exploring the Provision of Online Booter Services." *Deviant Behavior* 37 (10): 1163–78. https://doi.org/10.1080/01639625.2016.1169829.

Hyslip, Thomas S. 2020. "Cybercrime-as-a-Service Operations." In, edited by Thomas J. Holt and Adam M. Bossler, 815–46. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_36.

Hyslip, Thomas S., and Thomas J. Holt. 2019. "Assessing the Capacity of DRDoS-For-Hire Services in Cybercrime Markets." *Deviant Behavior* 40 (12): 1609–25. https://doi.org/10.1080/01639625.2019.1616489.

Jenny, Seth E., Margaret C. Keiper, Blake J. Taylor, Dylan P. Williams, Joey Gawrysiak, R. Douglas Manning, and Patrick M. Tutka. 2018. "eSports Venues: A New Sport Business Opportunity." *Journal of Applied Sport Management* 10 (1): 34–49. https://doi.org/10.18666/JASM-2018-V10-I1-8469.

Jones, Hattie, David Maimon, and Wuling Ren. 2017. "Sanction Threat and Friendly Persuasion Effects on System Trespassers' Behaviors During a System Trespassing Event." In, edited by Thomas J. Holt, 150–66. Routledge Studies in Crime and Society 26. London ; New York: Routledge, Taylor & Francis Group.

Kennedy, David M. 2012. *Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction*. 1st ed. Routledge. https://doi.org/10.4324/9780203892022.

Lau, F., S.H. Rubin, M.H. Smith, and L. Trajkovic. 2000. "IEEE International Conference on Systems, Man, and Cybernetics." In, 3:2275–80. Nashville, TN, USA: IEEE. https://doi.org/10.1109/ICSMC.2000.886455.

Leukfeldt, E. Rutger, Edward R. Kleemans, and Wouter P. Stol. 2017. "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks." *British Journal of Criminology* 57 (3): 704–22. https://doi.org/10.1093/bjc/azw009.

Maimon, David, Mariel Alper, Bertrand Sobesto, and Michel Cukier. 2014. "Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System." *Criminology* 52 (1): 3359. https://doi.org/10.1111/1745-9125.12028.

Miu, Tony, Ricky Yeung, Kitson Cheung, and Dominic Li. 2020. "Threat Report: Distributed Denial of Service (DDoS). Special Feature: COVID-19's Impact on the Online Gaming Industry." https://blog.nexusguard.com/threat-report/ddos-threat-report-2020-q3.

Müller, Kirill. 2020. *Here: A Simpler Way to Find Your Files*. https://CRAN.R-project.org/package=here.

Navarro, Jordana N., and Catherine D. Marcum. 2020. "Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime." In, edited by Thomas J. Holt and Adam M. Bossler, 527–45. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_18.

Newman, Graeme R., and Ronald V. Clarke. 2003. *Superhighway Robbery: Preventing e-Commerce Crime*. Cullompton: Willan.

Noroozian, Arman, Maciej Korczyński, Carlos Hernandez Gañan, Daisuke Makita, Katsunari Yoshioka, and Michel van Eeten. 2016. "Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service." In, edited by Fabian Monrose, Marc Dacier, Gregory Blanc, and Joaquin Garcia-Alfaro, 9854:368–89. Cham: Springer International Publishing. http://link.springer.com/10.1007/978-3-319-45719-2_17.

Pedersen, Thomas L. 2020. *Patchwork: The Composer of Plots*. https://CRAN.R-project.org/package=patchwork.

Pluss, Matthew A., Kyle J. M. Bennett, Andrew R. Novak, Derek Panchuk, Aaron J. Coutts, and Job Fransen. 2019. "Esports: The Chess of the 21st Century." *Frontiers in Psychology* 10 (January): 156. https://doi.org/10.3389/fpsyg.2019.00156.

Prichard, Jeremy, Richard Wortley, Paul A. Watters, Caroline Spiranovic, Charlotte Hunn, and Tony Krone. 2021. "Effects of Automated Messages on Internet Users Attempting to Access "Barely Legal" Pornography." *Sexual Abuse*, May, 107906322110138. https://doi.org/10.1177/10790632211013809.

R Core Team. 2022. *R: A Language and Environment for Statistical Computing*. Vienna. https://www.R-project.org/.

RStudio Team. 2022. *RStudio: Integrated Development Environment for r*. Boston, MA. http://www.rstudio.com/.

Ruiter, Stijn, and Frank Bernaards. 2013. "Verschillen Crackers van Andere Criminelen?" *Tijdschrift Voor*

Criminologie 55 (4): 342–59.

Schiks, Jim A. M., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. 2021. "Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right." Den Haag. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2021/een-alternatief-voor-jeugdige-hackers-361/.

Spitzner, Lance. 2003. *Honeypots: Tracking Hackers*. Boston: Addison-Wesley.

Steinmetz, Kevin F. 2015. "Becoming a Hacker: Demographic Characteristics and Developmental Factors." *Journal of Qualitative Criminal Justice & Criminology*, April. https://doi.org/10.21428/88de04a1.af131ffc.

Steinmetz, Kevin F., Thomas J. Holt, and Karen M. Holt. 2020. "Decoding the Binary: Reconsidering the Hacker Subculture Through a Gendered Lens." *Deviant Behavior* 41 (8): 936–48. https://doi.org/10.1080/01639625.2019.1596460.

Stockman, Mark, Robert Heile, and Anthony Rein. 2015. "An Open-Source Honeynet System to Study System Banner Message Effects on Hackers." In, 1922. Chicago, Illinois, USA: ACM Press. https://doi.org/10.1145/2808062.2808069.

Testa, Alexander, David Maimon, Bertrand Sobesto, and Michel Cukier. 2017. "Illegal Roaming and File Manipulation on Target Computers: Assessing the Effect of Sanction Threats on System Trespassers' Online Behaviors." *Criminology & Public Policy* 16 (3): 689726. https://doi.org/10.1111/1745-9133.12312.

Upadhyay, Ushma D., Iris J. Jovel, Kevin D. McCuaig, and Alice F. Cartwright. 2020. "Using Google Ads to Recruit and Retain a Cohort Considering Abortion in the United States." *Contraception: X* 2: 100017. https://doi.org/10.1016/j.conx.2019.100017.

Vetterl, Alexander. 2020. "Honeypots in the Age of Universal Attacks and the Internet of Things." https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-944.pdf.

Weisburd, David, Anthony Petrosino, and Trevor Fronius. 2014. "Randomized Experiments in Criminology and Criminal Justice." In, 4283–91. Springer New York. https://doi.org/10.1007/978-1-4614-5690-2_49.

Weulen Kranenbarg, Marleen, Stijn Ruiter, and Jean-Louis Van Gelder. 2021. "Do Cyber-Birds Flock Together? Comparing Deviance Among Social Network Members of Cyber-Dependent Offenders and Traditional Offenders." *European Journal of Criminology* 18 (3): 386–406. https://doi.org/10.1177/1477370819849677.

Wickham, Hadley, Mara Averick, Jennifer Bryan, Winston Chang, Lucy McGowan, Romain François, Garrett Grolemund, et al. 2019. "Welcome to the Tidyverse." *Journal of Open Source Software* 4 (43): 1686. https://doi.org/10.21105/joss.01686.

Wickham, Hadley, and Jennifer Bryan. 2019. *Readxl: Read Excel Files*. https://CRAN.R-project.org/package=readxl.

Wilson, Theodore, David Maimon, Bertrand Sobesto, and Michel Cukier. 2015. "The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace." *Journal of Research in Crime and Delinquency* 52 (6): 829–55. https://doi.org/10.1177/0022427815587761.

Wogalter, Michael S., and Christopher B. Mayhorn. 2008. "Trusting the Internet: Cues Affecting Perceived Credibility." *International Journal of Technology and Human Interaction* 4 (1): 75–93. https://doi.org/10.4018/jthi.2008010105.

Xie, Yihui. 2015. *Dynamic Documents with r and Knitr*. Second edition. Boca Raton: CRC Press/Taylor & Francis.

Xie, Yihui, Joseph J. Allaire, and Garrett Grolemund. 2018. *R Markdown: The Definitive Guide*. Boca Raton: Taylor & Francis, CRC Press.

Zhu, Hao. 2021. *kableExtra: Construct Complex Table with 'Kable' and Pipe Syntax*. https://CRAN.R-project.org/package=kableExtra.

A Appendix: Keywords

Table 4: List of 123 keywords related to DDoS attacks

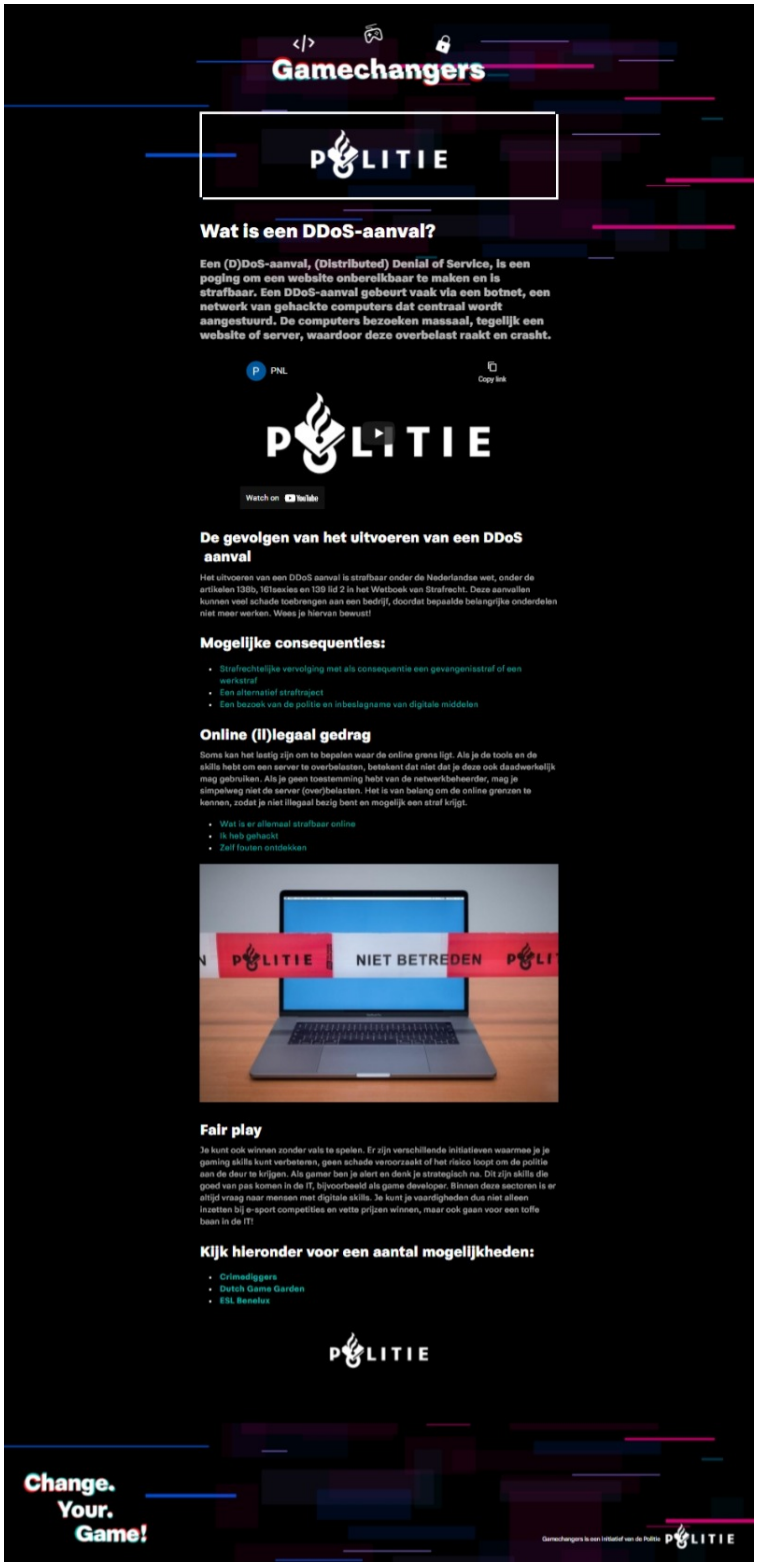
Keywords	Keywords	Keywords	Keywords
best ddos	ddos fortnite	ddos service	hoe werkt ddos
beste booter	ddos game	ddos skype	hoe werkt een botnet
beste stresser	ddos game account	ddos steam	how to ddos
booter ddos	ddos game server	ddos strafbaar	ip booter
booter free	ddos gamer	ddos stresser	ip booter free
booter gratis	ddos gaming	ddos tool	ip stresser
booter huren	ddos gratis	ddos tool huren	jahrein ddos
booter kopen	ddos handleiding	ddos tool kopen	kali dos attack
booter panel	ddos huren	ddos traceerbaar	kaspersky ddos
booter service	ddos influencer	ddos twitch	lan ddos
booter website	ddos internet thuis	ddos ubuntu	lizard stresser
botnet ddos	ddos ip	ddos website	minecraft ddos
botnet gebruiken	ddos ip adres	ddos windows	ps4 booter
botnet huren	ddos iptables	ddos youtube	python dos attack
botnet kopen	ddos kali linux	ddoser online	spel ddossen
botnet maken	ddos kopen	download booter	stresser huren
ddos aanval huren	ddos l7	download ddos	stresser kopen
ddos aanval kopen	ddos lan	download stresser	stresser service
ddos aanval uitvoeren	ddos league of legends	free booter	syn ddos
ddos apache	ddos linux	free ddos	test booter
ddos as a service	ddos livestream	free server	test ddos
ddos attack	ddos local	free stresser	test stresser
ddos call of duty	ddos magister	game ddossen	udp flood tool
ddos counter strike	ddos mirai	gamers booten	udp flooden
ddos cyberpunk	ddos online service	gamers ddossen	web stresser
ddos debian	ddos origin	gamers offline gooien	webstresser booter
ddos discord	ddos ping cmd	gamers stressen	webstresser free
ddos dos	ddos playstation	goedkope stresser	webstresser gratis
ddos esports	ddos pro	gratis booter panel	xorddos
ddos flood huren	ddos script	gratis stresser	zware ddos
ddos flood kopen	ddos server minecraft	hoe doe ik een ddos aanval	NA

B Appendix: Ad Designs

Table 5: Google Ads designs

Tone	Ad
deterrent (control)	Een DDoS-aanval is strafbaar | Gamechangers Ad publicaties.politie.nl/DDoS/attack Het plegen van een DDoS is strafbaar in Nederland onder het Wetboek van Strafrecht.
social	DDoS verpest het voor iedereen | Gamechangers Ad publicaties.politie.nl/DDoS/attack Dus je wilt dat je vrienden niet meer kunnen gamen omdat jij een grapje uithaalt?
informative	Wil je een game DDoS-en? | Gamechangers Ad publicaties.politie.nl/DDoS/attack Leer meer over DDoS-aanvallen en de impact hiervan op gamen.
reorienting	Play fair; verliezers DDoS-en | Gamechangers Ad publicaties.politie.nl/DDoS/attack Win eerlijk in een e-sport competitie door je gaming skills te trainen.

C Appendix: Landing Page Designs[5]



[5]Formal design: https://publicaties.politie.nl/changeyourgame/politie/; informal design: https://publicaties.politie.nl/changeyourgame/eslplay/

Gamechangers

ESL

Wat is een DDoS-aanval?

Een (D)DoS-aanval, (Distributed) Denial of Service, is een poging om een website onbereikbaar te maken en is strafbaar. Een DDoS-aanval gebeurt vaak via een botnet, een netwerk van gehackte computers dat centraal wordt aangestuurd. De computers bezoeken massaal, tegelijk een website of server, waardoor deze overbelast raakt en crasht.

Welke gevolgen zitten er aan het uitvoeren van een DDoS aanval?

Net als in andere landen waar ESL actief is, zijn ook in Nederland DDoS aanvallen strafbaar. Zeker wanneer er bewust schade wordt aangericht. Doordat onderdelen niet meer werken of tijdelijk onbereikbaar zijn kunnen deze aanvallen veel schade aanrichten aan personen en bedrijven. Hierbij kan je denken aan (professionele) gamers en game publishers. Wees je hiervan bewust!

Mogelijke gevolgen voor het inzetten van een DDoS aanval zijn:

- Strafrechtelijke vervolging met als consequentie een gevangenisstraf of een werkstraf
- Een alternatief straftraject
- Een bezoek van de politie en inbeslagname van digitale middelen

If you don't own it, you won't pwn it

Soms is het lastig om te bepalen waar online de grens ligt. Als je de tools en de skills hebt om een DDoS aanval te versturen, betekent dit niet dat je het zomaar mag doen. Als je geen toestemming hebt, mag je een server niet zomaar overbelasten. Het is dan ook belangrijk om online de grenzen te kennen, zodat je niet (onbewust) illegaal bezig bent en met Justitie te maken krijgt.

- Wat is er allemaal strafbaar online
- Ik heb gehackt
- Zelf fouten ontdekken

Copyright: ESL | Bart Oerbekke

Fair play?

Je kunt winnen zonder vals te spelen! Er zijn verschillende mogelijkheden waarmee jij je gaming skills kunt verbeteren, terwijl je daarbij geen schade veroorzaakt of de politie aan de deur krijgt. Als ESL weten we bovendien als geen ander dat je als gamer alert bent en strategisch nadenkt. Dit zijn eigenschappen die goed van pas komen in de IT, onder andere als game developer. Binnen deze sectoren is altijd vraag naar mensen met digitale talenten. Je kunt je vaardigheden dus niet alleen inzetten bij e-sport competities en vette prijzen winnen, maar ook gaan voor een toffe baan in de IT!

Kijk hieronder voor een aantal mogelijkheden:

- Crimediggers
- Dutch Game Garden
- ESL Benelux

ESL

Change. Your. Game!

Gamechangers is een initiatief van de Politie POLITIE