Silva, Karine; Roex, Ruben

Conference Paper

Zombie alert: Assessing legitimacy of P2P botnet mitigation techniques

25th European Regional Conference of the International Telecommunications Society (ITS): "Disruptive Innovation in the ICT Industries: Challenges for European Policy and Business" , Brussels, Belgium, 22nd-25th June, 2014

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Silva, Karine; Roex, Ruben (2014) : Zombie alert: Assessing legitimacy of P2P botnet mitigation techniques, 25th European Regional Conference of the International Telecommunications Society (ITS): "Disruptive Innovation in the ICT Industries: Challenges for European Policy and Business" , Brussels, Belgium, 22nd-25th June, 2014, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/101402

Zombie alert: assessing legitimacy of P2P botnet mitigation techniques

e Silva, Karine & Roex, Ruben[1]

1 PRIVATE SECTOR, INDIVIDUALS AND LAW ENFORCEMENT INTELLIGENCE GATHERING ON BOTNETS

1. This paper covers the legal analysis of crawling, a technically relatively advanced technique for gathering intelligence on a P2P botnet, a decentralised network of infected computers under the control of a bot master. The intel acquired via the crawling technique can subsequently be used to deploy mitigation techniques such as sinkholing, which disrupts botnet operations.[2] We have chosen crawling for its relevance in practice as well as the attention it has been given in scholarly discourse. In the following paragraphs, we present a high level overview of the technique's basic functionalities and requirements, before we perform a legal assessment of the legitimacy of the different aspect of this technique according to data protection and criminal procedure law.

1.1 MODUS OPERANDI OF A CRAWLER

2. Before we explain how this technique works, it is important to point out that this type of crawling should not be confused with the well-known and innocuous web crawling. A web crawler is used by, for instance, search engine providers to index the World Wide Web and is solely aimed at publicly accessible computer systems. A botnet crawler, however, looks for – as we shall see below – private computer systems that are only publicly accessible as a consequence of a successful botnet infection. This distinction between both types of crawlers has certain significant legal implications, at least with respect to the legality of the latter. But first, let us see how one deploys a crawler and what it does.

3. In order for someone to successfully deploy a crawler, certain preconditions will have to be fulfilled.[3] First, a working botnet crawler presupposes a detailed technical understanding of the malware installed on the individual infected systems. In practice this would mean that one has to reverse-engineer the malware to get a thorough understanding of its inner workings. Second, the initial deployment of the crawler requires that a few infected systems are known in advance. Third, the crawler needs to know the communication protocol used by the botnet in order for it to communicate with the infected machines. When all of these preliminary conditions are fulfilled and the crawler has successfully been developed, it can be deployed in the wild. The crawler will then visit the individual bots, will collect certain information on them and will ultimately provide a picture of *inter alia* the size of the botnet as well as the identity of the individual infected computer systems.[4] In a more formal way, one could describe the crawling technique as the automated iterative process of visiting bots, requesting their respective lists of known peers and

---

[1] Legal Researchers at the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE), Interdisciplinary Research for Law and ICT (ICRI), KU Leuven, iMinds.

[2] See for instance the recent attempt of Europol, the FBI and Microsoft to disrupt the ZeroAccess Botnet: Europol, "Notorious botnet infecting 2 million computers disrupted", December 2012, https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted-0.

[3] S. KARUPPAYAH, M. FISHER, C. ROSSOW and M. MÜHLHÄUSER, "On advanced monitoring in Resilient and Unstructured P2P Botnets", unpublished, 1-7, https://www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TK/botnetcrawling.pdf.

[4] D. DITTRICH, F. LEDER and T. WERNER, "A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets" in R. SION, R. CURTMOLA, S. DIETRICH, A. KIAYIAS, J.M. MIRET, K. SAKO and F. SEBÉ (eds.), *Financial Cryptography and Data Security*, Berlin – Heidelberg, Springer, 2010, 222-223.

enumerating the links between those peers. As it does nothing in terms of hampering 'normal' botnet operations, we could classify crawling as an intelligence gathering rather than a mitigation technique.[5]

4. In practice, companies and researchers in both academia and industry are the ones who mostly indulge in botnet crawling. However, recent initiatives indicate that law enforcement as well might be interested in incorporating this technique into their cyber arsenal.[6]

5. In this paper, we look at crawling as a technique against P2P botnets to examine two questions: 1. What are the legal grounds justifying the use of crawling by private sector and individuals, with special attention to data protection legislation; 2. What are the legal grounds justifying the use of crawling by law enforcement and their value in court. Due to our familiarity with the Belgian and Dutch legal systems, the analysis of the aforementioned questions is limited to the legal frameworks of Belgium and The Netherlands. Therefore, we look at the differences between both jurisdictions in dealing with the issues that arise when crawlers are used by private sector and individuals as an intelligence gathering technique and by law enforcement in a criminal investigation.

1.2 BOTNET MITIGATION BY PRIVATE SECTOR AND INDIVIDUALS

6. Today, private sector detains the control of most of our communications infrastructure and has therefore risen to be strategic players in promoting and ensuring security. In the past years, ever-growing interconnectivity and broadband penetration have not only amplified the risks and reduced the costs of malicious attacks, but also expanded the role of manufacturers and service providers as security actors. Looking ahead to the Internet-of-things, private sector is not only on the spotlight of the future of cyber security, but also hold the key to it. In addition to this, individual researchers and good-will security experts have often worked on their own. However, there are clear legal issues related to this type of activity, as well as to the private sector efforts in mitigating cyber crime. In this section, we explore the privacy and data protection issues related to the deployment of these mitigation tools by citizens and private sector and how can these operations be considered legitimate before the law.

1.2.1 Data Protection issues related to Crawling

7. From a data protection point of view, the main issues related to crawling are linked to the fact that this technique collects information about IP addresses while scanning the dynamics of the botnet. According to the position defended by the Article 29 Working Party in its Opinion 1/2008 on data protection issues related to search engines and reinforced by many national data protection authorities, the processing of IP addresses is to be considered as processing of personal data. This is the case unless the controller can prove he/she does not hold the reasonable means to identify the user behind the protocol. Even if the controller cannot reach the identity of the user, if the IP address is used in a way that allows the controller to single-out the user based on a pattern or behaviour, this will again fall within the scope of the EU data protection regulation.

8. If the processing involves personal data, the controller is not only required to abide to the data protection principles and ensure the opportune exercise of the data subject's rights, but also to justify its processing through one of the legitimate grounds set forth by Article 7 of the Data Protection Directive and implemented by national laws. However, before digging into which of these grounds could be used to justify the deployment of crawling techniques, the circumstances and environment surrounding the use of this solution need to be specified.

9. Because crawling only looks at traffic data and does not collect information related to the content of the messages, one could argue that it does not violate the confidentiality of the communications monitored. However, the current legal framework set forth by Belgian and Dutch legislator went ahead to protect the confidentiality of the metadata associated with communications. Furthermore, since crawling observes the connections and collects information about the population of the bot, it inevitably raises data

---

[5] *Ibid.*

[6] See for instance the presentation made by J. van Oss titled "EC3 Law Enforcement Action against Botnets" at Botconf 2013, https://www.botconf.eu/wp-content/uploads/2013/12/20-JaapvOss-Europol.pdf.

protection and unauthorized surveillance issues (as well as other specific criminal offences created by national law, such as unlawful obtaining/interception of data).

10. In order to analyse the legitimacy of crawling techniques, we need to answer two questions. The first relates to the identity of the controller, as the use of crawling by individual agents, computer security companies and ISPs has different outcomes. Therefore, defining which entity is monitoring which traffic is paramount. The second fundamental question is whether the agent using crawling technique is part to the communication or not. We look at all possible scenarios below related to three potential agents: individual agents, security experts acting on behalf of a security company/organization, and security experts acting on behalf of an ISP.

1.2.2 Crawling by an agent who is not part to a communication

1.2.2.1 Individual agent

11. It goes without saying that a good guy that, without being part to the communication, uses crawling techniques without the consent of the parties or authority to do so is acting unlawfully. In fact, this same person may not only violate the data protection rights of the parties (if he/she cannot prove that he/she does not possess the means and methods to attribute an identity to the user behind the identified device)[7], but also incur in criminal law offences created such as unauthorized surveillance, illegal obtaining of data and violation of confidentiality of communications.

1.2.2.2 Internet Service Provider

12. On the other hand, if a private sector agent that is not part to the communication (e.g. an ISP) crawls into a bot this monitoring can be justified if the agent has a legitimate interest in it. This legal door exists because service providers should be able to detect, filter and mitigate malicious traffic going under their own network. Under data protection laws, ISPs are able to mitigate threats affecting their networks through the combination of the Article 4 of the e-Privacy Directive and Article 7(c) of the Data Protection Directive, and the national laws that implemented the European legislation, as stated in the Article 29 Working Party Opinion 2/2006 on privacy issues related to the provision of email screening services. In The Netherlands, Article 11.2a(2) of the Telecommunication Act allows service providers to tap, listen in, intercept and monitor communications if these are necessary to preserve the integrity and security of their networks and services. In Belgium, Article 114 e-Communications law of June 13, 2005 brings a similar legitimate ground that can be used by ISPs.

13. Intelligence gathering techniques have been widely used by ISPs, as made possible by the legislator, and users are often made aware of these practices under the service terms and conditions. However, the use of mitigation technologies by service providers is restricted in both jurisdictions, as mentioned, as it is only allowed to the extent that it is essential to protect their services, performance, and securing the integrity of their customers and network. In the end of the day, this prevents ISPs from monitoring any traffic that is not related to their own IP range, or in other words, to indiscriminately mitigate malware in public networks.

1.2.2.3 Security companies

14. Clearly, there are several agents consistently crawling botnets on behalf of non-ISPs organisations. This is the case of security experts working for computer and Internet security companies. Here, there is no contract or legal duty to safeguard the network under attack or related to the IP range of the victims. Should this mean any intelligence gathering happening outside ISP networks is being conducted illegally? If there is no collection of personal data, there should be no infringement of data protection laws. But since crawling collects IP addresses of infected machines, it will invariably require the agent to abide to data protection standards, if he/she cannot prove this is not the case. We foresee one possibility in which this conduct can be legitimized in terms of data protection.

[7] It should be noted that this negative proof is hard to be achieved. Moreover, many DPAs may actually consider IP addresses as personal data by default, regardless of the identity of the agent behind the processing.

15. The only possible alternative we came across was for security companies to process infection data with the only purpose of defending the legitimate interest (e.g. fight against cybercrime, public security, network security, data integrity, etc.) of a third party (e.g. ISP), proven that this processing does not override the fundamental rights of the data subjects and is conducted in a proportional manner (Article 7(f) of Data Protection Directive; as implemented by Article 5(f), of Belgian Data Protection Law and Article 8(f), of the Dutch Personal Data Protection Act). This is to say that computer security experts can make use of Article 7(f) of the Data Protection Directive[8] to make their activities lawful, but this will only happen if: 1. All the processed data is relevant to a given ISP and is distributed to it, 2. There are enough safeguards in place reducing the impact of any potential drawbacks created by the crawling, 3. The agent is capable of conducting a concrete assessment of the balance of the third party legitimate interest and the impact of the crawling technique on the fundamental rights of data subjects. This would be the case if a computer security company crawls into a botnet with the sole intent of redistributing this information later on to the ISPs and network operators related to the range of infected IP addresses. Any additional disclosure, regardless of commercial purpose or compensation, to third parties that do not hold a legitimate interest will amount to a violation of the data protection legislation.

16. Finally, the proportionality principle must be fully integrated in the processing of personal data. According to the Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7, whoever makes use of the exception provided by Article 7(f) needs to concretely evaluate its impact on individuals and society, by taking into account the nature of the data processed, the status of the data subject and his legitimate expectations as well as the affected fundamental rights, the way the data are processed, and the balance of the gains expected from the processing, against the losses caused to others. The limits of the use of Article 7(f) are rather strict and may not be used as last resort. Although a legitimate ground exists, proving that fundamentals rights are balanced against the legitimate interest of the third party and the impact on the lives of data subjects is trickier than it sounds.

17. Furthermore, justifying the activities of security companies via Article 7(f) may not be sufficient to avoid prosecution for criminal law offences. Here, Belgian and Dutch laws differ. Article 124 of the Belgian e-Communications Law of June 13/2005 forbids anyone from collecting any data related to a communication in which he/she is not part to. However, Article 125(2) exempts the agent from such offence, as well as from incurring into Articles 259bis (violation of confidentiality of communications by public agents) and 314bis (violation of confidentiality of communications) of the Criminal Code, if the activity has the sole purpose of verifying the well functioning of the networks and to ensure the performance of the service. Since the legislator did not restrict the use of Article 125(2) to service providers, a security company that crawls into a botnet could possibly justify its activities under the aforementioned provision. This would be its strongest chance of avoiding prosecution for criminal offences under Belgian law. The same may not be the case under Dutch law, as no similar provision could be used to authorize crawling by non-ISP agents and avoid criminal prosecution, for instance, on the basis of Article 139c of Dutch Criminal Code.

1.2.3 Agent who is part to a communication

18. Whoever is part to a communication cannot be charged for unauthorized surveillance, as this offence necessarily asks for a third party to engage in such conduct. In any case, there could be specific criminal law offences created by national law that may classify crawling as a crime. In addition, an agent who is part to a communication may still violate data protection laws if he/she decides to crawl into a botnet without the consent of the parties or authorization to do so. This is because crawling into a botnet means collecting data not only from the offender, but also from several third parties (bots). Here the fact that the agent is part to the communication; a.k.a. is a bot himself, does not remove these data protection hurdles. Nevertheless, the condition of victim creates legal opportunities for the agent to lawfully mitigate the threat. The conditions analysed here do not change if the infection was unintended or intentionally pursued (e.g. via honeypots and other attracting techniques). First, we must again make a distinction based on the identity of the agent.

[8] While an individual agent could also try to justify his activities via Art. 7(f), we don't see how that reasoning would succeed in court or before a Data Protection Authority, since an individual is in a less accredited position to ensure the proportionality of the processing and the availability of safeguards that would guarantee potential drawbacks on the lives of individuals are kept to a minimum.

1.2.3.1 Individual agent

19. A good guy acting alone, even if part to a communication, still lacks a legitimate ground to deploy a largely privacy invasive technique such as crawling. As explained above, the fact that the agent is now part to the communication does not grant him/her the right to use the data of third parties nor will prevent legal prosecution in case his/her activities classify as criminal offences. A private agent may, for instance, avoid the data protection violation claim if he/she proves he/she has solely collected metadata that does not classify as personal data, because he/she does not possess the means to put a name and face on the persona behind the protocol. Therefore, the IP addresses could not be considered personal data and the activities would fall outside the scope of the data protection legislation, although this might be difficult to prove, as explained before. Furthermore, the legal issues involving criminal law are the same in the case the agent is not part to a communication.

1.2.2.2 Internet Service Provider

20. Because the law has granted significant room for ISPs to fight cybercrime affecting their own network, the fact that the ISP infrastructure has been directly targeted by the botnet only reinforces the right of the company to mitigate the threat. Here, the same legal grounds described in paras. 12 and 13 are applicable. Therefore, in the case an ISP crawls into a botnet that has infected clients on his network and directly targeted its infrastructure, it can lawfully use data related to the infection to mitigate the threat based on its duty to provide for the security of its operations, service, and integrity of its clients communications, as discussed before.

1.2.3.3 Security companies

21. The case of crawling by a security company is similar to the one of the individual agent: they both lack a legal duty to ensure security of the network and are not authorized to access the communication of third parties. In any case, a security company with solid reputation could make use of Article 7(f) of Data Protection Directive to legitimise its operations. The evaluation of whether the processing is in line with the exception created by Article 7(f) though can only be conducted individually and presents a significantly high threshold and a series of requirements that must be proved in concreto. Bringing a case based on Article 7(f), as discussed, is very tricky, but still the best solution at hand for companies that do not have a direct contractual relation with an infected machine and are not required by law to ensure the security of public networks. Finally, even when security companies would succeed in using Article 7(f) on their behalf, it is not yet clear whether they would be able to fully avoid prosecution under Belgian law. Under Dutch, this seems inevitable.

1.2.2.4 Crawling as self-defence

22. All three agents above, however, have the same right to defend themselves from the botnet if they find themselves in the condition of a bot. The use self-defence, a potential excuse precluding the unlawfulness of mitigation techniques, however, is rather limited and can only be verified case by case.

23. Because crawling itself if not capable of preventing or stopping the damage caused by a botnet, the use of crawling as a self-defence countermeasure can only be analysed as a first step towards botnet disruption or takedown. In any case, the use of crawling as part of a self-defence strategy can only take place if a legal right of the agent or a third party is being threatened by a conduct that amounts to a criminal offence. Since botnet infrastructures are used to perform cybercrimes affecting the integrity of data and information systems, self-defence could be used by any of the agents above to mitigate botnets in public networks. The use of self-defence, however, is limited to the deployment of reasonable force to stop or prevent a crime, and any excess in the use of this right is punishable. The countermeasure must then be proportional to the menace and timely exercised to prevent or stop the threat. Mitigating botnets on the basis of self-defence is thus challenging and may not be sufficient to exclude the unlawfulness of the technique in the case the disruption or takedown produces large-scale consequences to users, especially if these consequences could be reasonably expected by the agent before responding to the threat.

1.3 BOTNET CRAWLING IN A CRIMINAL INVESTIGATION: 4 DISTINCT ISSUES

1.3.1 Botnet crawling as a possible offence

24. As described in section 1.1, a crawler visits bots to retrieve information. It does so by exploiting the vulnerability caused by the botnet infection, issuing certain commands and relaying the information gained back to the person who deployed the crawler. Depending on the circumstances these distinct operations can be brought within the material scope of among others the legal provisions criminalising illegal access to computer systems (i.e. hacking) as well as those criminalising system and data interference, thus making botnet crawling a crime. Indeed, if one looks at the very broad conceptions of these criminal qualifications in both the Cybercrime Convention – after more than a decade still the primary international legal instrument in the area of computer crime – as well as the national implementations in Belgium and the Netherlands (both having ratified said Convention), one cannot escape the observation that the legal descriptions of these crimes are applicable to the use of a crawler.

25. Article 550bis, first paragraph of the Belgian Criminal Code (hereinafter: BCC) describes the crime of hacking as the accessing of or maintaining a presence in a computer system while knowing that one has no right.[9,10] Article 550ter, first paragraph BCC penalises he who – while knowing that he has no right – directly or indirectly enters, modifies or erases data in a computer system or with any other technological means changes the normal use of data within a computer system. Similarly, article 138ab of the Dutch Criminal Code (hereinafter: DCC) qualifies computer intrusion as deliberately and without right entering an automated work (for our purposes to be understood as a computer system) or a part thereof, while article 350a DCC penalises he who deliberately and without right modifies, erases, renders unusable or inaccessible data which are stored, process or transferred by means of an automated work or by means of telecommunication or adds data to them. The fact that a crawler accesses a computer system by exploiting the vulnerability caused by the botnet malware and issues commands to retrieve certain types of information brings it within the scope of these provisions. Moreover, given that general intent suffices for these crimes – implying quite a low threshold for criminalisation, as also foreseen in the Cybercrime Convention – one quickly risks criminal liability when deploying a crawler. The only way to avoid fines and/or even imprisonment is to show that in fact there is a right you can invoke to use an intelligence gathering tool such as a crawler.

26. Both in Dutch and Belgian law there are such rights to be found, rights that apply to several different kinds of entities. Private entities offering publicly available communication networks or public communication services, e.g. Internet access providers, have the legal obligation to take the appropriate technical and organisational measures to properly manage the risks for the security of their networks and services.[11] Hence, a tool allowing them to gather intel on a botnet that is threatening the stability of their networks due to a distributed denial of service attack and to contemplate an adequate mitigating strategy could be considered an appropriate technical measure. A similar argument can be made for operators of critical infrastructures that have a comparable obligation to manage security risks.[12] However, law enforcement is probably the type of entity you would naturally expect to have the competences necessary to use tools to gather intelligence on the public menace that is a botnet. So let us see which provisions they can count on the avoid criminalisation of their acts under the articles mentioned above.

27. First and foremost, we need to point out that neither Belgium nor the Netherlands have a competence which is particularly suited to legitimise botnet crawling. Rather, judiciary and police will have to rely on more or less traditional powers and apply them to the digital context. Three investigatory powers particularly stand out, which – at first sight – one might expect to cover the use of a botnet crawler. These are: intrusive surveillance, systematic surveillance and the network search. Intrusive surveillance, according to article 46quinquies, §1 of the Belgian Criminal Procedure Code (hereinafter: BCPC), is the power of a public prosecutor to authorise police officers to secretly – i.e. without the owner's knowledge or his

[9] All legal provisions cited are unofficial paraphrased translations from the authors. Note that we do not attempt to give an exhaustive list here (one might for instance also think of the prohibition of taking note of the existence of communication, i.e. the protection of meta-data) of possible criminal qualifications, we simply want to indicate that crawling is only possible for those who can invoke a legitimate ground for doing so.

[10] The equivalent provision in the Cybercrime Convention is to be found in article 2.

[11] Article 114 Act 13 June 2005 concerning electronic communications, *BS* 20 June 2005, 28070.

[12] Article 13, §1 Act 1 July 2011 concerning the security and protection of critical infrastructures, *BS* 15 July 2011, 42320.

consent – enter a private place when there are serious suspicions that the punishable facts constitute a crime of a certain severity or are committed within the remit of a criminal organisation, and no other investigatory means seem to suffice to uncover the truth. The private place cannot be a home, a part of a home or an office of a doctor or lawyer. The rest of the article then goes on to list the conditions and modalities of intrusive surveillance, which we will look into later on. The Dutch Criminal Procedure Code (hereinafter: DCPC) has a comparable provision in articles 126k or 126r, which hold that the public prosecutor can order in the interest of the investigation that an investigator without prior authorisation of the right holder enters a private place, excluding a home, or uses a technical means in order to inspect the place, safeguard traces or install a technical means to record the presence or moving of an item. The conditions under which either 126k or 126r DCPC can be used depend on the case, but that will be covered later on.

28. Systematic surveillance is another investigatory competence, yet arguably farther reaching in terms of infringing on a person's right to privacy. Article 47sexies, §1 BCPC foresees that (systematic) surveillance is the systematic observation by police officers of one or multiple persons, their presence or conduct, or of certain items, places or circumstances. The surveillance is considered systematic when (a) it stretches for five consecutive days or more than five non-consecutive days spread out over the period of a month, (b) it involves the use of technical means, (c) it has an international character, or (d) it is undertaken by specialised units of the federal police. The Dutch equivalent can be found in article 126g DCPC which states that the public prosecutor can order an investigator in the interest of the investigation to systematically follow a person or to systematically observe his presence or conduct.

29. The third investigatory power that at face value seems relevant is the network search, which is much more tailored to the digital reality than the previous two. In essence it is a competence that allows law enforcement to extend an initial search in a computer system to connected systems. The Belgian variant of this power has been enshrined in article 88ter BCPC, which holds that when an investigatory judge (notice that in principle it is no longer the public prosecutor who is competent) orders a search in a computer system or a part thereof, this search can be extended to a computer system or part thereof which is at a different location. Such a search is only possible if this extension is necessary to uncover the truth of the crime subject to the investigation, or if other measures would be disproportional, or if there is a risk that without such extension pieces of evidence would be lost. The Dutch variant of this power is to be found in article 125j DCPC, which holds that one can extend a search (initiated on the basis of article 125i) to data stored in an automated work located somewhere else, if these data are reasonably necessary to uncover the truth. If such data are found, they can be recorded. However, with regard to crawling relying on the network search does not seem possible, for the simple reason that both under Belgian and Dutch law, the extension is only possible to systems to which people authorised to use the initial system subjected to the search have access to. In the context of crawling a botnet, this would mean that if law enforcement has the authority to initiate the crawling technique starting from a known infected computer only person A is entitled to using, it can only crawl systems to which A legitimately has access. In the context of a botnet, A most likely does not have access to other infected computers, which bars law enforcement from relying on the network search to crawl these other systems. Hence, the network search cannot be used to legitimate crawling.

30. In the next three sections we will cover three more issues related to crawling, allowing us to assess whether the two remaining investigatory powers can actually legitimise the use of a botnet crawler by law enforcement. We will also look into some legal developments in The Netherlands that may be more suited to this end, remediating some of the issues we will identify along the way.

31. One final remark still needs to be made regarding the possible criminal character of the act of deploying a botnet crawler. Earlier we indicated that a crawler could only be developed if one has a thorough understanding of the botnet malware used to infect the individual computers. This implies that the law enforcement agents, who wish to investigate a certain botnet, either reverse engineer the malware and build the crawler themselves, acquire knowledge on the botnet malware and then build the crawler themselves, or simply acquire the crawler they need for deployment. Each of these possibilities could be qualified as the crimes of developing, owning or acquiring hacking tools or malware (articles 550bis, §5 and 550ter, §4 BCC and article 139d, 2, a DCC). The Belgian text, however, expressly foresees that this is only the case if this development, ownership or acquisition happens without right. Hence, as we do below,

we must investigate whether law enforcement does indeed have a right to develop, acquire and/or own such tools.

1.3.2 Deploying a botnet crawler only makes sense when it is done covertly

32. Several botnets have intelligent detection and mitigation capabilities that hinder the workings of a crawler, thus strongly limiting its usefulness.[13] Hence, crawling only makes sense when it remains under the radar. However, not every investigatory power can be used covertly, given the greater impact on a person's fundamental rights, especially the right to privacy (as *inter alia* enshrined in article 8 of the European Convention on Human Rights, hereinafter: ECHR, and as described above). Both intrusive surveillance and systematic surveillance are investigatory competences which allow explicitly for covert law enforcement action under the conditions outlined in the respective provisions of the Criminal Procedure Code, thus providing a strong basis in law fulfilling the requirements of *inter alia* article 8, paragraph 2 ECHR. Therefore, the covert aspect of botnet crawling seems covered by both of these powers.[14]

1.3.3 Deploying a crawler as a 'technical means'

33. The qualification of a crawler as technical means in the context of a criminal investigation has immediate implications for the applicability of certain investigatory powers. Especially for intrusive surveillance and for systematic surveillance one should assess whether the crawler can be considered a technical means, given that both these investigatory powers were initially created with only the physical world in mind, not the virtual world. Hence, it might take some creative and evolutionary legal reasoning to apply these powers in the digital context.

1.3.3.1 Crawling as an intrusive surveillance technique

34. The wording of both Belgian and Dutch provision on intrusive surveillance alludes on an application in the physical world rather than the virtual. The preparatory legislative work of the Belgian provision, for instance, only cites examples of physical private places.[15] But the opinions in doctrine on whether this competence can in fact be used in a digital setting vary both between and within jurisdictions, which should not come as a surprise seeing how the wordings of the provisions subtly differ.[16] Nevertheless, an evolutionary interpretation of the existing provisions will be necessary, given that these are already over a decade old.

§1 Intrusive surveillance under Belgian law

35. If we first consider the Belgian situation, it should be noted that article 46quinquies, §4 BCPC – for the moment making abstraction of the use of intrusive surveillance as a preparatory phase for systematic surveillance – could be construed as a way of applying article 46quinquies in the digital realm. Indeed, paragraph 4 of said article states that using technical means for the purposes of assessing what is present at the location in terms of items related to the (intended) crime or profits gained from committing the crime (article 46quinquies, §2 BCPC), as well as collecting evidence of the presence of such items, can be equalled with entering a private place for the same purposes (article 46quinquies, §1 BCPC). If we want to apply this to the deployment of a botnet crawler for the purposes of gathering intelligence on a botnet, we will need to assimilate the infected computer with a private place and to qualify the deployment of a crawler as using a technical means.

Crawling private places

36. VAN LINTHOUT and KERKHOFS argue that private parts of the internet can be assimilated with the concept of a private place in the sense of article 46quinquies, §1 BCPC, considering that the wording of

---

[13] See *supra*, footnote 3, p. 2.

[14] Note that with regard to the network search, some authors argue that covert use of this competence is not possible considering that requirements of article 8, paragraph 2 ECHR are not fulfilled. In this sense: C. CONINGS and J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?", *Computerrecht* 2013, Vol. 1, 23-32.

[15] Wetsontwerp houdende diverse wijzigingen van het Wetboek van Strafvordering en van het Gerechtelijk Wetboek met het oog op de verbetering van onderzoeksmethoden naar het terrorisme en de zware georganiseerde criminaliteit, *Parl.St.* Kamer 2005-06, nr. 2055/001.

[16] See *infra*.

the provision does not exclude application in cyberspace.[17] However, where the authors discuss a situation where private places are still virtually located in publicly accessible cyberspace (e.g. a private profile on Facebook), we are looking at the situation where the private place would be assimilated with a private computer, made accessible only by the vulnerability caused by the botnet malware. It might be that this private computer is located at home or in the office of a doctor or lawyer, which makes one wonder whether crawling such computers is not excluded by article 46quinquies, §1, second paragraph BCPC (see marginal 27). If a private computer located at home yet connected via the internet is deemed to be part of the home, one cannot rely on article 46quinquies BCPC, but should rather rely on article 89ter BCPC which enshrines the intrusive surveillance within the judicial investigation under the authority of the investigating judge instead of the public prosecutor. The rationale behind this different approach for private places and homes, is that the legislator deemed the impact on a person's private life far greater when searching a home (which is also protected by article 15 of the Belgian Constitution) than some other private place.[18] Hence, the more stringent safeguards of article 89ter BCPC apply when indeed a home is to be the target of the intrusive surveillance.

37. The difficulty in the context of botnet crawling is of course that you do not know in advance which types of machines will be crawled. To that extent it is a random process. We would argue, however, that for the purposes of botnet crawling, article 46quinquies could still be used indiscriminately of the type of the machine being crawled and this for two reasons.

38. First of all, with the connected reality of today, it does not make sense – in terms of virtual accessibility – to determine the protection worthy character of the machine through its physical location. An individual might for instance host a website on his home computer, making it to an extent publicly accessible even if it is at home.[19] Moreover, it creates a weird and illogical discrepancy between e.g. portable computers and smartphones on the one hand and desktop computers on the other. The former category of devices will indeed often be found outside the home, but they are – given the information they contain – often very protection worthy. Therefore, one should differentiate between the virtual parts of the computer where personal content is stored which should be heavily protected, and those (technical) parts that are virtually accessible as a consequence of networking functionalities.

39. Secondly, considering that the different treatment of homes vis-à-vis private places and public places is based on the degree of infringement upon a person's private life and his right to the protection of his home, it would make sense to bring crawling within the remit of the public prosecutor's investigatory competence under article 46quinquies BCPC. Indeed, the violation of a person's private life when his computer is being crawled is fairly small, considering that the crawler only looks for IP-addresses and links between machines in relation to the botnet's operations. It is by no means interested in a person's private data stored on the individual device. Hence, we would argue that the infected computer is a private place – albeit virtual – in the sense of article 46quinquies BCPC to the extent that it is accessible for crawling. The argument that it is not publicly accessible place is of course rooted in the observation that the individual device is only accessible due to the malware infection.

Deployment of a crawler as using technical means[20]

40. Technical means under Belgian law are defined in the provision on systematic surveillance as a configuration of components which detects signals, transports them, activates their registration and registers these signals, with the exception of those means which are used to execute a digital wiretap.[21] Signals are every event provable via a technical means.[22] These definitions do not seem incompatible with the use of a crawler. Yet, since crawling qualifies as hacking in the sense of article 550bis BCC (see

[17] P. VAN LINTHOUT and J. KERKHOFS, *Cybercrime*, Brussel, Politeia, 2013, 242-243. See also: C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon* 2012, 219-220.

[18] Wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/01, p. 57.

[19] Note that the Belgian Court of Cassation with its decision of 21 October 1992 seems to hold that only private parts of the home are protected, parts that are open to the public are not protected by article 15 of the Belgian Constitution: see B. VANGEEBERGEN, "Inkijkoperatie" in A. VANDEPLAS, P. ARNOU and S. VAN OVERBEKE (eds.), *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2007, p. 39. If we apply this reasoning to the virtual context, it would mean that only the private parts of the computer are protected, not the public ones.

[20] See also *infra*, marginal 46.

[21] Article 47sexies, §1, third indent BCPC.

[22] See *supra*, footnote 18, p. 32.

marginal 25), it implies that under the Belgian conception of intrusive surveillance law enforcement can be authorised to use hacking tools in order to gain remote access to computer systems. It consequently also absolves law enforcement from the crime of developing, acquiring or owning hacking tools or malware (see marginal 31). VAN LINTHOUT and KERKHOFS metaphorically refer to such use of hacking tools as a kind of digital locksmith.[23]

§2 Intrusive surveillance under Dutch law

41. The Dutch provisions on intrusive surveillance allow for much less leeway and evolutionary interpretation according to several authors.[24] OERLEMANS argues that given the intrusiveness of remote hacking – which is an integral part of crawling as we saw earlier – one cannot and should not extend the initial physical conception of intrusive surveillance that far in light of the infringement upon an individual's right to privacy (art. 8 ECHR).[25] In our opinion, this view is a bit too indiscriminate regarding the different types of hacking and their impact on a person's private life. Similarly as we argued under Belgian law, the crawler's impact is fairly limited, considering that it only looks at the existence of the (technical) communication in a botnet and the machines involved but does not go further. Of course, would the crawler indeed access an individual's content on the infected computer, the infringement would be far greater and the privacy argument would hold.

42. More convincing is the legal technical argument made by KOOPS and BURUMA.[26] They compare intrusive surveillance with the competence of the intelligence services to access an automated work in order to capture data as introduced by the 2002 Act on intelligence- and security services, which came about around the same time as the Act on Special Investigatory Powers inserted intrusive surveillance into the DCPC. Since the legislator did create an explicit competence for intelligence services, but did not do the same for law enforcement in the DCPC, one should conclude that the legislator did not deem it appropriate for law enforcement to have such a competence. In our opinion, this argument is backed by the legal developments in the Netherlands with the so-called Act Computer Crime III, which expressly foresees a competence for law enforcement to hack but is still undergoing the legislate process.[27] Considering that the legislator only now contemplates introducing a police competence to hack, implies that such a power does not currently exist within the Dutch criminal legal framework. Hence, under the DCPC intrusive surveillance cannot be used to allow botnet crawling.

1.3.3.2 Crawling as a systematic surveillance technique[28]

§1 The systematic nature of crawling

43. Above (marginal 28) we summarised the four circumstances that give surveillance under article 47sexies its systematic nature. In a botnet crawling context, no less than three of those grounds apply, namely (b) the use of technical means, (c) the international character, and (d) undertaken by specialised units of the federal police. With regard to the technical means, we refer to what we discussed under intrusive surveillance and what follows in section §2 below.[29]

44. When one crawls a botnet, it is impossible to know in advance where each of the machines being crawled is located. Unless one restricts the IP range the crawler is allowed to search and access (which would to a large extent incapacitate the crawler in the first place), the crawler might very well move through cyberspace and access infected computer all over the globe. Hence, law enforcement use of a botnet crawler at face value will always have an international character. Under the fifth and final issue

---

[23] See *supra,* footnote 17, p. 243.
[24] See *inter alia* J.J. OERLEMANS, "Hacken als opsporingsbevoegdheid", *DD* 2011, 901-903 who cites also: B.W. SCHERMER, *Opsporing vs. Privacy in peer-to-peer netwerken,* 's Gravenhage, Sdu Uitgevers, 2003, 53; B.J. KOOPS and Y. BURUMA, "Formeel strafrecht en ICT" in B.J. KOOPS, *Strafrecht en ICT,* Den Haag, Sdu Uitgevers, 2007, p. 118.
[25] See J.J. OERLEMANS, *supra*, footnote 24.
[26] See B.J. KOOPS and Y. BURUMA, *supra* footnote 24.
[27] Proposed article 125ja in Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit, http://www.internetconsultatie.nl/computercriminaliteit.
[28] It should be noted that, seeing that the argument made in marginal 42 is true for systematic surveillance in the Netherlands as well, it has no added value to describe its application for crawling in detail here. We will therefore limit ourselves to an analysis of the Belgian conception of systematic surveillance. Also note that there is a similar distinction between systematic surveillance of a private place (art. 47sexies BCPC) and systematic surveillance of a home (art. 56bis BCPC) as there was for intrusive surveillance, but since the arguments for qualifying crawling as the one or the other are the same, we will not go into it here.
[29] See *supra*, marginal 40.

regarding crawling (section 1.2.5) we will touch briefly upon this important but highly complex issue of the borderless nature of crawling.

45. As indicated earlier, deploying a crawler requires significant technical knowledge and will probably require the intervention of the specialised police units who have such expertise. In Belgium it would most likely be the National Technical Support Unit (NTSU) who would in fact be able to deploy a crawler. The NTSU is part of the CGSU or specialised units of the Belgian federal police. Its main tasks are technical and tactical placements of technical means (e.g. placing a bug for wiretapping), R&D and operational support by for instance concealing certain technical tools and data management.[30]

§2 Technical means and cyberspace

46. VAN LINTHOUT and KERKHOFS point out that the concept of 'technical means' in the context of an observation (or intrusive surveillance for that matter) in the virtual world does not really work.[31] Indeed, in order the access cyberspace in the first place one will always need a computer, which – according to the broad definition in article 47sexies BCPC (marginal 40), qualifies as a technical means making any cyber observation systematic. The authors argue, however, that the computer in such a setting should be seen as mere sense-enhancing tool such as binoculars. Moreover, insofar the use of specialised software is not decisive for the ability of observing but only needed for the dealing with the observation, the authors deem such software not to be a technical means either. If this reasoning is applied to the deployment of a botnet crawler, one must conclude that the crawler is a technical means in the sense of article 47sexies BCPC. Indeed, the ability to observe is completely defined by the crawler's functionality: its very essence is to acquire intelligence and thus to observe. The crawler is no mere access portal to the medium being observed but the technical means to conduct the systematic surveillance when access to the medium has already been established (i.e. a governmental computer with an internet connection).[32]

§3 Relationship with intrusive surveillance

47. We have now argued that under Belgian law, materially both intrusive surveillance and systematic surveillance appear to cover to an extent the deployment of a crawler by law enforcement. We now need to see how both these competences relate to one another in the context of crawling. In our opinion, they each cover a different phase. The initial phase, i.e. the construction of the crawler by recreating the malware, determining the communication protocol and accessing the initial bots by exploiting the botnet malware so as to start the crawling, can be construed as intrusive surveillance since one accesses a private place to place a technical means for the purposes of systematic surveillance later on.[33] As soon as the crawler is effectively deployed in that it starts returning peer lists and visiting other infected machines following its own process, the conditions for systematic surveillance become fulfilled and a mandate on the basis of article 47sexies BCPC will be required.

1.3.4 Crawling knows no borders

48. With the growing popularity of cyberspace globally and especially the emergence of cloud computing, the level of interconnectedness of individual devices has skyrocketed. This has led to a strange discrepancy between the physical and virtual world, where the former is governed by borders and thus necessarily national sovereignty, and the latter is seemingly borderless allowing one to digitally move across the globe instantaneously. In criminal procedure law especially this discrepancy has profound implications as it creates a crippling disadvantage for law enforcement vis-à-vis the cybercriminals. Indeed, law enforcement competences are very much defined in terms of (physical) territorial authority emanating from state sovereignty, while cybercriminals move about without these territorial restrictions.

49. With respect to the competences described above, we should therefore analyse whether crawling by Belgian law enforcement, which is also borderless since most botnets span the entire globe and limiting the crawling to a territorially defined IP-range would therefore make no sense, can include devices in other

---

[30] See among others: Federale politie, "Speciale eenheden leveren al 40 jaar onbaatzuchtig en doeltreffend werk", March 2012, p. 2, http://www.polfed-fedpol.be/org/pdf/053-2012N_40%20jaarCGSU.pdf.

[31] P. VAN LINTHOUT and J. KERKHOFS, *supra* footnote 17, p. 248.

[32] Note that the authors argue that the internet itself is also not a technical means, but a mere medium in which the actual systematic surveillance will take place.

[33] Art. 46quinquies, §2, 3° BCPC.

territories.[34] Law enforcement agents deploying a crawler will probably only be able to ascertain the location of the infected devices on the initial list needed to start the crawling. From then on, they have no means to determine in advance in which jurisdictions their crawler will end up. Does this mean that they should simply refrain from crawling, because they might infringe upon the sovereignty of another state? VAN LINTHOUT and KERKHOFS defend the opinion that searching on the Internet is so different from searching in the physical world, that the concept of territoriality should be reinterpreted for cyberspace.[35] They hold that from the moment you are able to make a certain observation from Belgian territory, without having to physically move abroad, the surveillance is to be situated in Belgium. Therefore, if Belgian law enforcement is authorised by mandate for systematic surveillance and deploys the crawler in Belgium, the systematic surveillance takes place in Belgium since they receive the crawling results on Belgian territory.

50. Whether this reasoning will be followed by the Belgian courts and accepted on the international level remains to be seen, since it virtually does away with the principal of sovereignty in cyberspace. Indeed, it places individuals in other countries at the mercy of foreign law enforcement. According to this reasoning, any law enforcement agency in the world that is allowed to crawl under its national legislation would be able to claim that it is only conducting an investigation on its own territory. This would open the door to governments everywhere hacking individuals' devices in other countries potentially without due regard for their fundamental right, all under the guise of legitimated national surveillance.

1.4 CONCLUSION

51. The data protection hurdles faced by individuals, security companies and service providers when deploying crawling techniques are significantly different, as the Belgian and Dutch legislator have created distinctive grounds to legitimate mitigation activities by private sector and individuals. As discussed, an individual agent acting on his own behalf is invariably committing criminal offences, in addition to potential data protection violations. The case of security companies is not very different, with the exception that these agents are in a better position to make use of special provisions created by the legislator, such as Article 7(f) of Data Protection Directive and Article 125(2) of Belgian e-Communications Law. Here the main factors to be taken into account are the safeguards put in place by the agent to enable a fair balance between the fundamental rights of the data subjects and the legitimate interested pursued. Nevertheless, companies crawling in public networks are potentially committing criminal offences under Belgian law and invariably incurring in such under Dutch law. Finally, ISPs are the only agents that can lawfully make use of crawling techniques without infringing data protection and criminal laws, within the limits created by the legislator, due to their duty to ensure the security of the processing of data, as well as the security of their networks, integrity of its customers, and performance of the contracted service. The use of crawling as self-defence, as examined, also presents several issues that may not be sufficient to preclude the unlawfulness of the use of the technique when the agent is not legally authorised to do so.

52. With regard to law enforcement competences to deploy a botnet crawler, both under the Belgian and Dutch Criminal Procedure Code it seems impossible to deploy a crawler on the basis of the network search. For the Netherlands crawling even seems impossible altogether under the currently applicable legal framework. If and when the proposal for an Act Computer Crime III gets signed into a law, crawling will most likely be possible from a material point of view as a form of legitimated law enforcement hacking, but the territorial implications of crawling might prevent it from being admissible in practice. In Belgium the different phases of crawling – from initialisation to deployment – are materially covered by intrusive surveillance and systematic surveillance respectively. However, the cross-border nature of crawling makes it hard to defend in terms of national sovereignty and territorially defined jurisdiction. Some authors claim that territoriality should apply differently in the context of systematic surveillance in cyberspace, opening the door for law enforcement use of botnet crawlers. However, we doubt whether such broad interpretation of Belgian jurisdiction in cyberspace can be maintained on an international level.

---

[34] Since we have already established that the Netherlands currently does not have an investigatory power to support crawling and that the network search does not apply, we will only look into the possibility of cross-border use of intrusive and systematic surveillance under Belgian law.
[35] P. VAN LINTHOUT and J. KERKHOFS, *supra* footnote 17, p. 249-250.