Legal Implications of Countering Botnets

Joint report from the
NATO Cooperative Cyber Defence Centre of Excellence
and the
European Network and Information Security Agency (ENISA)

Liis Vihul[1], Christian Czosseck[2], Dr. Katharina Ziolkowski[3],
Lauri Aasmann[4], Ivo A. Ivanov[5], Dr. Sebastian Brüggemann, M.A.[6]

Information security specialists have developed various techniques and methods to reduce the threat that botnets pose to the security of information systems connected to the internet. The implementation of such methods needs to take place according to the legal systems of the respective jurisdictions. Based on Estonian and German legislation, the authors cover two different approaches to support the fight against botnets: first, a legal evaluation is given to common technical measures used to fight botnets, primarily relating to botnet takeover and takedown; second, some purely legal constructs, such as compensation for unlawfully caused damage, are suggested, which could potentially apply to certain circumstances and so indirectly contribute to the mitigation of botnets. As a result, a number of legal requirements, as well as potential risks, relevant in the fight against botnets are outlined.

[1] Legal Analyst at NATO Cooperative Cyber Defence Centre of Excellence.
[2]At the time of writing this article, Scientist at NATO Cooperative Cyber Defence Centre of Excellence.
[3] Scientist at NATO Cooperative Cyber Defence Centre of Excellence.
[4] Legal and Policy Branch Chief at NATO Cooperative Cyber Defence Centre of Excellence.
[5] Attorney-at-law and General Corporate Counsel of eco – Association of the German Internet Industry.
[6] Post-graduate civil service trainee at eco – Association of the German Internet Industry.

The authors would like to express their gratitude to Ms. Monika Mikiver (Office of the Chancellor of Justice of Estonia) and Ms. Kerttu Tänav (MA University of Tartu) for their contribution to this report.

Notice must be taken that the opinions expressed in this publication are those of the authors and should not be considered the official position of the NATO Cooperative Cyber Defence Centre of Excellence, NATO or ENISA.

Introduction

Botnets, networks of compromised or hijacked computers, have been around for more than two decades. Over the last years, however, accelerated by the expansion of the internet and the massive increase of internet-connected services, as cyber crime has become increasingly organised, botnets have turned into a major and multifaceted underground industry generating huge profits for cyber criminals. They are used for malicious activities, such as massive information theft, spam campaigns and the execution of distributed denial of service (DDoS) attacks, rendering the targeted services unavailable. Furthermore, botnets have been involved in many of the most large-scale cyber attacks the world has witnessed to date, such as the DDoS attacks against Estonia in 2007 and Georgia in 2008,[7] as well as being employed by hacktivists to convey their messages.

On a daily basis, information security specialists use various techniques to detect and mitigate botnets; however, there seems to be a great deal of uncertainty as to what are the requirements and restrictions arising from the law which should be considered with respect to each technique. To that end, this report discusses some of the most common

[7] See, e.g., *Tikk, E., Kaska, K., Vihul, L.* International Cyber Incidents: Legal Considerations. CCD COE Publishing, Tallinn, 2010.

botnet-fighting methods from a legal perspective, in order to address the potential legal concerns and risks related to each of them.

After a brief introduction to botnets, the report gives an overview of the development of the European Union criminal legislation relevant to the fight against botnets. Then, anti-botnet techniques and methods are analysed in the context of the legislation of two European Union Member States, Germany and Estonia. With Germany representing a big European Union founding nation known for its strong protection of basic rights, privacy in particular, on the one side, and the small country of Estonia being a fairly recent member of the EU, known for its IT-innovativeness and flexibility, on the other, two quite different countries have been selected for this study.

Even though the analysis relies primarily on Estonian and German law, it should be kept in mind that Estonian as well as German information society legislation is largely based on that of the European Union and that cyber offences in the respective Penal Codes were developed taking into account the requirements set forth in the Council of Europe Cybercrime Convention.[8] Therefore, many of the problems which are addressed and their proposed solutions can be quite universal, especially in the context of the European Union.

This report tries to point out most of the potential points of concern related to the technical measures used to counter botnets, as well as the responsibilities of various affected stakeholders arising from different areas of the law. The complexity of countering botnets is to a great extent caused by the very fact that many areas of law become relevant and have to be viewed and analysed holistically. Although not covered in this report, a number of examples of botnet takedowns and takeovers already exist in different jurisdictions, and the experience gained from these case studies, specific to each individual botnet, should also be taken into account when planning a botnet takedown or takeover. The practical knowledge from past cases combined with the academic approach of this report, as well as appropriate and timely legal advice, should help to ensure the lawfulness of anti-botnet operations.

The prospective audience for this report is not limited to representatives of the legal profession who are requested to advise on certain anti-botnet measures, but is also expected to include information technology specialists involved in, or considering, infiltrating, taking down or taking over a botnet. Keeping in mind the interdisciplinary readership of this study, it is written so that no specialist knowledge of either discipline is required in order to follow the logic of the discussions.

Botnets

A ‘botnet’, a term derived from the words ‘robot’ and ‘network’, is a network of

[8] Council of Europe, Convention on Cybercrime. ETS no. 185. Budapest, 23.11.2001. Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

interconnected, remote-controlled computers generally infected with malicious software turning the infected systems into so-called ‘bots’, ‘robots’ or ‘zombies’.[9;10] Bots are remotely controlled by one or many malicious actors, commonly referred to as ‘botherders’ or ‘botmasters’. While having complete control over the bots, the botmaster is able to execute basically any action the legitimate owner[11] of the computer could carry out.

Botnets are mostly commanded to do the following:[12]

1. Locate and infect other information systems with malware. This functionality, in particular, allows botmasters to maintain and build their supply of new bots to enable them to undertake, among others, the functions below.
2. Conduct distributed denial of service attacks.[13]
3. Rotate IP addresses under one or more domain names for the purpose of increasing the longevity of fraudulent websites, which are used, for example, for hosting phishing and/or malware sites or command and control (C&C) servers of botnets.[14]
4. Send spam, which in turn can distribute more malware.[15]

[9] See, e.g., *Leder, F., Werner, T., Martini, P.* Proactive Botnet Countermeasures – An Offensive Approach. In *Czosseck, C., Geers, K.* (Eds.). The Virtual Battlefield: Perspectives on Cyber Warfare. Amsterdam: IOS Press, 2009, p. 211.

[10] See, e.g., OECD Working Party on Information Security and Privacy (WPISP) in partnership with the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG). Malicious Software (Malware): A Security Threat to the Internet Economy. Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, OECD Ministerial Meeting on the Future of the Internet Economy. Seoul, Korea, 17-18 June 2008, p. 22.

[11] Throughout this report the term ‘owner’ appears. However, it is not intended to demonstrate the actual ownership of the computer in question in terms of property law, but to refer to the lawful possessor of the device, be it the owner or some other person who has gained the right to possess it.

[12] *Supra nota* 10, p. 22.

[13] A denial-of-service attack (hereinafter: DoS attack) or distributed denial-of-service attack (hereinafter: DDoS attack) is an attempt to make a computer resource unavailable to its intended users, generally consisting of the concerted efforts of a person or people to prevent an internet site or service from functioning efficiently or at all, temporarily or indefinitely. DoS attacks are, therefore, primarily aimed at disrupting the availability of computer system resources to authorised users, usually by sending invalid data that causes the server software to crash. The increasing amount of spam can also cause a DoS by decreasing or denying availability of email services to authorised users and by clogging their mailboxes with unwanted emails, thus interfering with the user's ability to send and receive legitimate email messages. To launch DDoS attacks, cyber criminals commonly use botnets in an attempt to flood the victim's network with requests and disrupt access to the target Web site or to overload the victim's servers and cause them to crash. – *Hansche, S. et al.* Official Guide to the CISSP Exam 3-8. 2004, pp. 155-156.

[14] In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. – *Ollmann, G.* The Phishing Guide: Understanding and Preventing Phishing Attacks. Available at: http://www.technicalinfo.net/papers/Phishing.html

[15] Spam describes the emission of unsolicited bulk messages. Although various scams exist, the most common is email spam. Offenders send out millions of emails to users, often containing advertisements for products and services, but frequently also malicious software. Today, organisations providing email services report that as much as 85 to 90 per cent of all emails are spam. – MAAWG Tackles Bots with New ISP Guidelines for Restoring Infected End-Users’ Machines. Available at: http://www.maawg.org/media_center/maawg-tackles-bots-with-new-isp-guidelines-for-restoring-infected-end-users-machines

5. Steal sensitive information from compromised computers that belong to the botnet.
6. Host the malicious phishing site itself, often in conjunction with other members of the botnet to provide redundancy.

In most cases, the goals of the attackers tend to be focused on financial gain. It is estimated that botnets generate an income of 10,000 to 10,000,000 USD per month per botnet.[16] Seeing these numbers helps one to understand why malware is now a global criminal industry and also gives an indication of how many resources can be invested into developing new, more sophisticated malware that is more resistant to detection or mitigation efforts. As a result, an underground botnet business has emerged, whereby botnets are used as a service that can be bought, customised or rented.

Additionally, politically motivated botnet attacks are on the rise and have gained international attention. In 2007, botnets were used to launch DDoS attacks against Estonian governmental and private sector websites. During the Russo-Georgian conflict in 2008, botnets were used to limit Georgia's possibilities to distribute information regarding the on-going military conflict to the Georgian public and the outside world. Botnets are also an easily accessible tool for hacktivists to use to make or support a statement, be it of a political or other nature.

There are two principal strategies for an attacker to acquire a botnet: either to buy or rent an existing botnet from the black market or to deploy one by himself. The latter typically requires the botmaster to conduct four major steps.

First, the attacker needs to obtain the software of the two most important components of the botnet: the bot client[17] and the C&C server. The attacker can either develop and build those by himself or use available open-source botnet software. The third option is to buy a so-called botnet construction kit. For the ZeuS botnet,[18] the basic construction kit, including the C&C server component, can be bought for about 3,000 to 4,000 USD. Additional features to harden the ZeuS botnet against takedown attempts or latest exploits needed to overcome even well-protected computers can be bought in the form of 'add-ons'. Prices for these depend on the provided feature set, but they commonly price up to 10,000 USD.[19]

[16] See, e.g., *Menn, J.* Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet. PublicAffairs, 2010; Villeneuve, N. KOOBFACE: Inside a Crimeware Network. November 2010. Available at: http://www.infowar-monitor.net/reports/iwm-koobface.pdf

[17] A bot client is a piece of malware which infects computers often without their owners' knowledge and approval, turning them into remotely controlled machines accepting and executing any command given by the C&C server. Together with the latter, they form a botnet.

[18] There is no single Zeus botnet, but the toolkit is a commercial product that is available on the internet to anyone interested. Therefore, the number of Zeus botnets is probably quite large. Of the different botnet software, the Zeus toolkit is perhaps the best known and widely used. – Macdonald, D. Zeus: God of DIY Botnets. Fortinet. Available at: http://www.fortiguard.com/analysis/zeusanalysis.html; Lemos, R. Microsoft Lawsuit Names Two Responsible for Zeus Botnet Attacks. eWeek.com, 2 July 2012. Available at: http://www.eweek.com/c/a/Security/Microsoft-Lawsuit-Names-Two-Responsible-for-Zeus-Botnet-Attacks-138938/.

[19] *Stevens, K., Jackson, D.* ZeuS Banking Trojan Report. Available at: http://www.secureworks.com/research/threats/zeus

As the second step, the botmaster needs to set up the C&C infrastructure consisting of at least one, but often multiple, C&C server instances spread over multiple internet service providers (ISPs) to enhance the botnet's robustness against takedown attempts. Sometimes, additional inactive C&C servers are operated to guarantee access to the botnet even after a coordinated takedown action has rendered the visible C&C infrastructure unavailable.

This core infrastructure is commonly extended by a set-up of additional servers providing, for example, the following functionalities. Some of these services are deployed on hijacked computers rather than on those possessed by the botmaster:

a) An FTP server[20] (or similar service) to maintain files used in the process of infecting new computer systems and to distribute later versions of the bot client in the course of updating the infected hosts;
b) A 'drop zone', to which the bots send the information stolen from the infected computer;
c) Websites used for phishing attacks or for infecting new computers.

It is important to note that the design of a botnet depends on the creativity and skills of the botmaster, which is why botnets vary greatly as to their level of sophistication and resistance to takedown attempts.

After the preparations are complete, the botmaster needs to successfully infect an initial set of computers. Initial infection may occur in several different ways; for example, in a case where the host has a certain vulnerability, a malicious program exploits the vulnerability and runs on the host. "Malware can also be automatically downloaded while viewing web pages, executed through opening an email attachment or a computer can be infected by USB auto run."[21] Furthermore, hackers often deceive users into downloading software to their computers as part of a seemingly innocent software package, such as a screen saver, game, or some utility program, or attempt to lure unsuspecting users to visit web sites or click on hyperlinks that will install malware on their machines.[22]

Updating existing software, including anti-virus software (and even having it in the first place) helps mitigate this risk significantly. Nevertheless, even up to date anti-virus solutions find it difficult to detect malware with a sufficient level of certainty. Sometimes, the detection rates of new malware within the first 24 hours are less than 10% and they

[20] The File Transfer Protocol (FTP) is a commonly used network protocol used to transfer files of all kinds over networks, especially the internet. It is based on a client-server architecture, where the FTP server provides files for FTP clients to access them on request.

[21] *Zhu, Z. et al*. Botnet Research Survey. 32nd Annual IEEE International Computer Software and Applications Conference 2008, pp. 967-972. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4591703

[22] *Ena, M*. Securing Online Transactions: Crime Prevention Is the Key. Fordham Urban Law Journal, Vol. 35, no. 1, p. 158.

seldom exceed 90%.[23] Modern worms[24] only need a few hours to spread to all reachable systems across the globe.

The next phase in the botnet setup process is secondary infection and maintenance. After a successful infection, the bots will connect back to the C&C server waiting for the botmaster's orders. If commanded, the bots will scan actively for vulnerable computers within their reach and will infect them automatically; or they will update themselves with later versions of the bot client software to enhance their capabilities or to patch vulnerabilities. This way the botmaster maintains a steady number of reachable, up-to-date bots for his free disposal.

The global infection rate of computers is difficult to measure. Microsoft, for example, measured an average global infection rate of 7.1 out of 1000 computers as a result of cleaning them with Microsoft's free malware remover in the second quarter of 2011.[25] This number is probably too low, as not every owner of a Windows system is using this software and malware detection rates in general are not high, but nevertheless the figures still give an initial impression. The Shadowserver Foundation, a group of voluntary security experts tracking botnets, detected about 5500 different botnets in February 2012.[26] This clearly illustrates the fact that the potential damage of botnet attacks in enormous.

To sum up, botnets have turned into powerful tools for both criminals and politically motivated actors.[27] At the same time, setting up and operating a botnet is relatively easy, considering the availability of instructions and tools. Low computer security awareness or ignorance of computer users supports the rapid spreading of new malware, although even well-secured and patched computer systems are not resistant to the latest malware. Anti-virus companies find it difficult to cope with the enormous stream of new malware every day.

It is therefore obvious that botnets need to be fought against and the task of the legal community is to define the legal framework for this action. A number of technical and non-technical mitigation techniques have been developed over time; however, often they are difficult to execute due to constraints of, or uncertainty about, the law applicable to the mitigation process. The mitigation techniques will be introduced in the following sections and analysed with regard to their lawfulness according to the laws of Estonia and Germany.

[23] See, e.g., Detection rate of popular anti-virus products. Available at: http://www.shadowserver.org/wiki/pmwiki.php/Stats/Virus60-DayStats

[24] A worm is a special type of malware capable of and intended to self-replicate and spread further without any user intervention.

[25] Microsoft Security Intelligence Report, Vol. 12, July through December 2011. Available at: http://www.microsoft.com/security/sir/default.aspx

[26] Shadowserver Foundation. Botnet Charts. Available at: http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts

[27] Famous examples of botnets include Agobot (2002); Spybot, Rbot, Sinit (2003); Beagle, Bobax (2004); Rustock, ZeuS (2006); Pushdo, Storm, Cutwail, Srizbi (2007); Asprox, Kraken, Mega-D, Torpig, Conficker, McColo (2008); BredoLab, Grum, Maazben (2009); Waledac (2010); Kelihos, BlackShades (2011).

European Union Policy and Regulatory Background – Moving Towards the Criminalisation of Botnet-Related Activities

Network and Information Security

Initiatives of the EU relevant to the fight against botnets fall into the larger context of EU actions concerning the information society as a whole. They comprise the EU legal framework[28] as well as the instruments with no binding effect on Member States. This section will give a brief overview of how these initiatives, which directly and mostly indirectly deal with botnets, have shaped the EU landscape concerning botnets into what it is today and what are the expected results of the current developments taking place in the EU.

In its 2001 Communication,[29] "Network and Information Security: Proposal for A European Policy Approach", the EU distinguished three different, but interrelated, policy areas as relevant for tackling security challenges for the information society: the already existing telecommunications and data protection frameworks; cyber crime policies; and the to-be-developed network and information security (NIS) measures, which would address the growing concerns of cyber espionage and cyber attacks potentially also threatening national security.[30] NIS is defined as "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems"[31]. The birth of a coordinated European policy on NIS marked the realisation that a new domain of national security had evolved and needed to be addressed accordingly.[32] In the years 2004-2006, a coordinated EU policy approach towards critical infrastructure protection was developed and the first legislation on critical information infrastructure protection (CIIP) was adopted in 2009.

[28] EU law or community law means the set of rules adopted by the European Community. Community law consists mainly of the Treaties and the instruments adopted by the institutions under the Treaties, such as Regulations and Directives. The case-law of the Court of Justice is also one of the sources of Community law.

[29] A Commission Communication is a policy document with no mandatory authority. The Commission takes the initiative of publishing a Communication when it wishes to set out its own thinking on a topical issue. A Communication has no legal effect. – http://ec.europa.eu/civiljustice/glossary/glossary_en.htm

[30] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach. COM(2001)298, p. 3.

[31] *Ibid.*, p. 9.

[32] An interesting example illustrating how the EU reached the recognition that network and information security in general was a new domain, which needed unconventional approaches, is the following. In 2000 the state of mind regarding securing networks was that since these measures are costly, arbitrary solutions could not be imposed and it is up to the market to define the adequate level of security (eEurope 2002 An Information Society For All. Action Plan prepared by the Council and the European Commission for the Feira European Council. 19-20 June 2000. COM(2000)330, p. 10.). However, by 2001 this attitude had already changed, as the Commission voiced the view that "certain market imperfections lead to the conclusion that market forces do not drive sufficient investment into security technology or security practice" (*Supra nota* 30, p. 19).

Whereas electronic communications, data protection, cyber crime and CIIP are independent areas with corresponding legal instruments, NIS, instead of a separate category, should be seen as the overarching policy framework that strives to achieve a holistic approach to the new security challenges.[33] Therefore, it can be said that EU legislation dealing with the information society falls into three categories, all, at least to an extent, under the umbrella of the NIS policy:

1. regulatory framework for electronic communications and data protection;[34]
2. instruments dealing with cyber crime;
3. CIIP measures.

From the perspective of countering botnets, all three are important as they ensure the criminalisation of malicious activities conducted via botnets, the availability of log files for investigations, the protection of personal data during investigations, the existence of information-sharing and cooperation mechanisms, etc. Threats posed specifically by botnets have impelled considerable legislation in recent years, but in the context of spreading malware they were mentioned already in 2006.[35] In that timeframe, the criminal use of botnets started gaining significant momentum; but even before 2006, EU documents frequently noted the disruptive effects of denial of service attacks, requiring the Union's attention and reaction.

Cyber Crime

The issue of cyber crime was first brought onto the high-level agenda of the EU in 1999, when the Tampere Summit of the European Council[36] concluded that effort should be spent on agreeing on common definitions, incriminations and sanctions in sectors of particular relevance, one of them being high-tech crime[37]. This guidance was followed in

[33] This view does not necessarily correspond with how the EU would categorise these areas. For example, in 2007 the Commission explained: "It is hard to draw an exact dividing line between the area of network and information security and the area of fight against cyber crime, since no effective crime repression policy can be established without an effective prevention and general security policy supporting it, and vice versa." (Impact Assessment Report SEC(2007)0642, accompanying Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime, COM(2007)267). Since NIS is, as the Commission itself stated, the "prevention and general security policy", and impacts legislation not only dealing with cyber crime, but also electronic communications, data protection and CIIP, it is more natural to place all of the aforementioned areas under the NIS umbrella.

[34] Although in the context of NIS the EU prefers to consider them together, they could also be viewed as two separate categories.

[35] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society – "Dialogue, partnership and empowerment". COM(2006)251, p. 4

[36] The European Council comprises the Heads of State or Government of the Member States and it meets at least four times a year. The role of the European Council is to provide the European Union with the necessary impetus for its development and to define the general political guidelines, but it does not exercise any legislative function. – http://europa.eu/legislation_summaries/glossary/european_council_en.htm

[37] In the EU, the terms 'cyber crime', 'computer crime', 'computer-related crime' and 'high tech crime' have been used as synonyms, especially at the beginning of the previous decade. Today, however, referring to 'cyber crime' appears to be the prevalent practice.

2000 in the European Council and Commission's[38] eEurope 2002 Action Plan, which called for a better coordination to fight cyber crime – a new form of crime using the tools of the information society. Economic damage caused by disruptions in internet functioning, for example by denial of service (DoS) attacks, was said to be on the rise.[39] Since there are alternatives to botnets to conduct DoS attacks, the attacks which caught the attention of drafters were not necessarily launched via botnets. However, as a result of this recognition system interference was eventually criminalised and this would cover the conduct, irrespective of the tools used. The Action Plan foresaw that a coordinated and coherent European approach to cyber crime would be established by the end of 2002.

In early 2001, the Commission released a Communication on creating a safer information society by improving the security of information infrastructures and combating computer-related crime.[40] In it, the Commission promised to bring forward a legislative proposal to approximate cyber offences in national laws, emphasising that the criminalisation of hacking and DoS attacks was particularly important. Furthermore, the proposal would introduce standard definitions for the EU in this area. The Commission proposal of June 2001 on a European policy approach to network and information security already confirmed that the aforementioned legislation would be developed.[41] As a result, in April 2002 the Commission presented a proposal for a Council framework decision[42] on attacks against information systems. Meanwhile, the terrorist attacks of 9/11 had forced the EU to revise its strategic approach to international terrorism. This affected the planning of the framework decision as well, making it a priority that the criminal legislation of member states would be prepared to handle cyber terrorism.

The harmonisation of substantive criminal law through the framework decision was to ensure that national legislations were to a critical extent homogenous and therefore equally prepared to support the prosecution of transnational cyber crimes by enabling cooperation between Member States' law enforcement and judicial authorities. Approximation of criminal law also helps to avoid forum shopping, whereby criminals choose to act in Member States where their actions are not criminalised at all, or have

[38] The European Commission's main function is to propose and implement Community policies adopted by the Council and the Parliament. It acts in the general interest of the Union with complete independence from national governments. It enjoys a quasi-exclusive right of initiative in matters where the Community method applies (matters where Member States have transferred a significant part of their responsibilities, such as the Common Agricultural Policy, the Customs Union, the internal market, the Euro, etc.), which drive European integration. – http://europa.eu/legislation_summaries/glossary/european_ commission_en.htm

[39] eEurope 2002 An Information Society For All. Action Plan prepared by the Council and the European Commission for the Feira European Council. 19-20 June 2000. COM(2000)330, p. 10.

[40] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. COM(2000)890.

[41] *Supra nota* 30, pp. 25-26.

[42] Before the adoption of the Lisbon Treaty, under Article 34(2)(b) of the Treaty on European Union, framework decisions were used to approximate the laws of Member States similarly to directives. They were binding upon the Member States as to the result to be achieved, but left to the national authorities the choice of forms and methods. The institute of a framework decision was abolished when the Lisbon Treaty came into force.

less severe sanctions. To that end, the proposal for the framework decision foresaw the criminalisation of two malevolent acts: illegal access to information systems and illegal interference with information systems. It took three years for the European community to finally adopt the framework decision[43] and in it the latter crime was broken into two different articles, thereby introducing three provisions, which all Member States were supposed to incorporate into their national laws:

- Article 2 – Illegal access to information systems
- Article 3 – Illegal system interference
- Article 4 – Illegal data interference.

'Illegal access' means access without right to the whole or any part of an information system, thereby protecting the confidentiality of information systems. 'System interference' covers the intentional serious hindering or interruption of the functioning of an information system by manipulating[44] with computer data; and 'data interference' covers the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system. Illegal system interference is particularly a provision which addresses denial of service attacks. Hacking, on the other hand, would either fall under illegal access to information systems or illegal data interference, depending on the nature of the concrete action. To ensure a consistent approach in its application, the framework decision provided definitions for the terms 'information system' and 'computer data'. It also obliged Member States to sanction illegal system and data interferences by criminal penalties of a maximum of at least between one and three years of imprisonment. Member States were required to take necessary measures to comply with the provisions of the framework decision by March 2007.

In late 2006, the Commission noted botnets in its 'Spam Communication'[45] as the medium to send spam emails, referring to an estimation that botnets relay over 50 per cent of abusive emails. In May 2007, the Commission issued yet another document on cyber crime, a communication aiming to establish a general policy roadmap to improve European and international level coordination in the fight against it.[46] In the communication, botnets were pointed out as increasingly prevalent vehicles for conducting large-scale attacks, whether against information systems, individuals, organisations or nation states. It recognised that cyber attacks can also be directed against European critical infrastructures, potentially entailing disastrous consequences for the whole society.[47] Although not a novel statement to make, this time it was influenced by a

[43] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[44] 'Manipulating' is a word used by the author to cover all activities listed in Article 3: 'inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data'.

[45] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software. COM(2006)688, p. 3.

[46] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime. COM(2007)267, p. 3.

[47] *Ibid.*, p. 2.

real-life cyber incident and not only a hypothetical threat – the large-scale distributed denial of service attacks targeted against Estonia in April-May 2007. The communication also reassured that harmonising Member States' criminal legislation continues to remain a long-term objective of the EU.[48]

The framework decision was followed by an assessment report from the Commission to the Council on its implementation in July 2008.[49] The assessment report pointed out that Member States had implemented the penal legislation in diverse ways; however, it also highlighted that despite the differences, the level of implementation was relatively good. More importantly, due to the fact that the European community had recently been shocked by the attacks against Estonia, the assessment report also started paving the way for new EU legislation which would be prepared to effectively handle threats specifically arising from the exploitation of botnets. The report hinted that the criminalisation of activities facilitating the criminal use of botnets as well as tougher minimum penalties for system interference were considered. Before the EU released its proposal for new legislation on cyber crime, it also mentioned botnets in its CIIP initiative. The Commission Communication on CIIP said that botnets were a threat to nations' critical information infrastructure, as illustrated by the examples of Estonia and Georgia, and had to be tackled accordingly.[50]

The Botnet Directive

At the end of September 2010, the Commission issued a proposal for a directive on attacks against information systems,[51] colloquially usually referred to as the 'Botnet Directive', which, when adopted, will repeal the framework decision on attacks against information systems. The directive's overall goal is to "deter the occurrence of, and decrease the number of large-scale attacks originating from and/or targeting the EU"[52] by prosecuting and convicting criminals and improving cross-border cooperation between law enforcement agencies. However, the provisions as proposed by the Commission are subject to change in the legislative procedure. For example, the European Economic and Social Committee,[53] in its opinion on the Commission's proposal, calls for even more stringent penalties, so that their severity would reflect the seriousness of the crime as well

[48] *Supra nota* 46, p. 8.

[49] Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems. COM(2008)448, p. 10.

[50] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". COM(2009)149, pp. 4, 7.

[51] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. COM(2010)517.

[52] Commission Staff Working Document Impact Assessment Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA. SEC(2010)1122, p. 21.

[53] The European Economic and Social Committee is a consultative body of the EU which integrates social and economic interest groups. Its 344 members are nominated by national governments for a term of five years. The Committee's task is to issue opinions on matters of European interest to the Council of the European Union, to the European Commission and to the European Parliament.

as act as a realistic deterrent to criminals.[54] More generally, the Committee emphasises the importance of adopting a comprehensive and forward-looking approach, dealing not only with law enforcement and punishments, but also with prevention through better security measures, detection and education, the latter by increasing investment in research and development.[55] The Committee proposes to bring internet security under centralised control, whereby a central authority would establish standards for foolproof terminal devices and network, website and data security.[56]

The proposal for the directive explains that the shortcomings of the already existing provisions in the framework decision are, first, that they do not fully address the potential threat of botnets, and second, that they do not take sufficient account of the gravity of the crimes and their sanctions.[57] To tackle the identified deficiencies, the proposal introduces two new basic offences. Illegal interception criminalises the interception of non-public transmissions of computer data. The second offence aims at penalising the production, sale, procurement for use, import, distribution or otherwise making available of a computer program, intended to also cover the notion of a botnet, to commit the crimes in the directive. It will also criminalise malevolent trading with passwords, access codes and similar data.

With regard to penalties, generally the maximum term of imprisonment will be at least two years. However, if system or data interference is committed against a significant number of computer systems, as in the case of a botnet attack, the maximum term of imprisonment will be at least three years. The most severe penalty, a maximum term of imprisonment of at least five years, is foreseen on three occasions: system or data interference which is committed within the framework of a criminal organisation causes serious damage or is committed against critical information infrastructure.

Furthermore, the directive seeks to improve European cooperation in criminal matters by strengthening the existing structure of 24/7 contact points,[58] including an obligation to provide feedback within eight hours to urgent requests. The feedback may also be negative, denying help to the requestor – the important thing is that feedback is received relatively quickly. The directive also requires Member States to collect statistical data on cyber crimes, such as the number of offences registered and the number of persons prosecuted and convicted for the offences as they stand in the directive.

[54] Opinion of the Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, 4 May 2011, point 1.10

[55] *Ibid.*, point 1.5.

[56] *Ibid.*, point 1.6.

[57] *Supra nota* 51, p 5.

[58] Article 35 of the Council of Europe Cybercrime Convention foresees that the Signatories shall "designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence".

Member States will be obliged to transpose the directive's provisions into their national legislation no later than two years from its adoption. Considering that it will take a while until the directive is finally adopted by the European Union, and from that moment the Member States will have another two years to comply with its provisions, the effects of the directive can be assessed only after some years. The directive will have accomplished its goals and even more if, first, it achieves its direct goal to tackle the threat posed by botnets, but second, its provisions are abstract enough so that they will also easily apply to new, similar forms of cyber crime, which today are yet unknown to us and will emerge in the future.

EU Legislation and the Council of Europe's Cybercrime Convention

A relevant concern regarding EU activities in the fight against cyber crime is how they align with the Council of Europe Convention on Cybercrime,[59] also known as the Budapest Convention, which was opened for signature in 2001 and entered into force in 2004. As of today, the Convention has been signed by 47 nations, including all 27 EU Member States, and ratified by 32. Of those 15 countries which have not ratified the Convention, 9 are Member States of the European Union. The Budapest Convention has three goals: to harmonise domestic criminal substantive law, to provide domestic criminal procedural law with the necessary powers to investigate and prosecute cyber crimes, and to set up a fast and effective regime of international cooperation.[60]

The EU has considered the Cybercrime Convention in every initiative it has launched; however, the positions that the EU has expressed vary from emphasising the Convention's necessity and encouraging states to join it, to demonstrating the Union's disappointment at the low number of ratifications during the rather long period in which the Cybercrime Convention has been in force, and recognising the need for alternative instruments. The eEurope 2002 Action Plan, adopted in the year 2000, already mentioned that Council of Europe was discussing a convention on cyber crime and emphasised the importance of ensuring discussion and cooperation on this issue.[61] In the same year, the Union saw the need for approximation of criminal law at the EU level, but the intention from the beginning was to build its efforts on the Cybercrime Convention.[62] In the communication laying down the general policy for fighting cyber crime, the Commission encouraged Member States which had not yet ratified the Convention – "the predominant European and international instrument in this field" – to do so.[63] Also, the proposal for the framework decision stated that the framework decision would be consistent with the approach taken in the Cybercrime Convention.[64]

[59] *Supra nota* 8.

[60] Explanatory report to the Convention on Cybercrime. Chapter III, point 16.

[61] *Supra nota* 39, p. 11.

[62] *Supra nota* 40, p. 15.

[63] *Supra nota* 46, p. 6.

[64] Proposal for a Council Framework Decision on attacks against information systems. COM(2002)173, p. 8.

The 2010 Stockholm Programme put some pressure on Member States, calling on them to ratify the Budapest Convention as soon as possible.[65] This encouragement was repeated in the proposal for the 'Botnet Directive', where the Commission also modestly shared its disappointment at the low number of ratifications by Member States.[66] Although the Commission was pursuing new legislation with its proposal, which, when adopted, would lose the need for Member States to ratify the Convention, the Commission still spurred Member States to do so. This was probably an attempt simply to prevent setting the two instruments in contrast, and probably also bearing in mind the fact that it would take many years before the EU legislation would be adopted. The impact assessment accompanying the proposal stated that any EU action has to consider existing instruments in order to avoid duplication of effort.[67] However, a close examination of the 'Botnet Directive' proposal and the Cybercrime Convention shows that, as far as substantive criminal law is concerned, the proposal very slightly differs from the Convention. The two biggest weaknesses of the Convention in the eyes of the EU are the non-effectiveness of the existing 24/7 contact points and the fact that the Convention does not specifically address large-scale attacks,[68] and it has therefore introduced measures to relieve these deficiencies in the proposal.

As mentioned, Article 35 of the Budapest Convention requires all parties to designate a point of contact, which is available on a twenty-four-hour, seven-day-a-week basis, and all of which together form the 24/7 Network. However, it does not establish any obligations regarding the procedure to be followed when assistance is sought. In contrast, the EU proposal requires that urgent requests must be dealt with in eight hours, although the answer to the request may also be negative. The second, most notable, difference between the Convention and the Directive proposal is the fact that the EU will prescribe concrete penalties for all offences, whereas the Convention only prescribes that sanctions be effective, proportionate and dissuasive, which may, but does not have to include the deprivation of liberty.

From the EU's perspective, in addition to the aforementioned changes the Directive will introduce, another important benefit is that those nine Member States who have chosen not to ratify the Cybercrime Convention will nevertheless be obliged to amend their legislation once the Directive enters into force. Since the Directive will have all of the substantive law elements of the Convention and more, the goal to harmonise EU legislation will be reached. Although the EU has chosen to take advantage of the legislative powers it possesses, for the rest of the world the Cybercrime Convention has not lost its value and importance. Despite being drafted more than a decade ago, it continues to be an effective and the most authoritative tool in fighting cyber crime, and joining it should be brought onto the agendas of all the nations who have not yet done so, in order to successfully prosecute international cyber crimes.

[65] The Stockholm Programme – An open and secure Europe serving and protecting citizens. 2010/C 115/01, point 4.4.4.

[66] *Supra nota* 51, pp. 3-4.

[67] *Supra nota* 52, p. 5.

[68] *Ibid.*, p. 21.

Estonia and Germany have both signed and ratified the Cybercrime Convention. In addition, their legislations are to a great extent homogenous in the areas of law which are harmonised at the European Union level, such as electronic communications, e-commerce and personal data protection. How the provisions, as set forth in the Cybercrime Convention and European Union legislation, are transposed into the respective national legal systems, and how they are interpreted in the context of countering botnets, is illustrated below.

Fight Against Botnets – Touching the Limits of Existing Laws

Inspection of Packet and Traffic Records

If a computer or a computer network is suspected of or known to be infected with botnet software, one of the first and logical steps, besides applying anti-virus software, should be routine or ad hoc packet and traffic data inspection and analysis to detect and characterise botnet traffic. This is a passive technique to identify the existence, extent and behaviour of botnets in order to determine if and what further action is needed to disable the botnet software or preferably to take down the entire botnet. This technique is commonly used in corporate environments connected to the internet as well as by internet service providers.

At first it is important to note that a distinction must be made as regards which entity is monitoring which traffic. Depending on these circumstances, slightly different legal issues may arise, mostly due to the mandate that each entity is given. Generally, the seemingly harmless and routine technical action of inspecting packets and traffic is surrounded by a number of legal concerns, most notably those of personal data protection, unauthorised surveillance and confidentiality of communications.

Perspective of breaching criminal law

From a criminal offence viewpoint, one aspect to take into consideration when analysing the applicability of norms dealing with cyber crimes is that most of the provisions in the Estonian Penal Code took effect only in 2008, whereas in Germany the first criminal law reform related to computer crimes took effect in 1986[69], the latest in 2007 by the 41th Penal Code Reform Act for the fight against computer crime.[70] For this reason, convictions in Estonia are limited and most of the respective analysis is merely theoretical and not yet backed up with court practice. Nevertheless, packet and traffic

[69] Second Law to combat economic crime (Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)), BGBl I, 721; with further annotations in BT-Drs. 10/318. First introduction of 'data espionage' § 202a German Criminal Code and 'data manipulation' § 303a German Criminal Code; see Laue, in: jurisPR-StrafR, 13/2009, Anm. 2.

[70] Criminal Law Amendment Act to combat computer crime (Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄG)), BGBl 2007 I, 1786; with further annotations in BT-Drs. 16/3656 and BT-Drs. 16/5449.

inspection may also fall under the more traditional crimes, such as unauthorised surveillance.

If a person in Estonia is monitoring traffic for botnet fighting purposes, the main danger lies in the fact that such monitoring might be regarded as illegal surveillance under the respective criminal law provisions of the Estonian Penal Code.

> *§ 137. Unauthorised surveillance*
> *(1) A person without the lawful right to engage in surveillance who observes another person in order to collect information relating to such person shall be punished by a pecuniary punishment or up to 3 years' imprisonment.*[71]

This provision presumes intentional collection of information relating to a specific person.[72] Although § 137 of the Penal Code was not initially drafted in light of cyber activities and the main use of this regulation has been the physical observance of another person, the scope of this section could be extended so that it becomes relevant in the cyber context. In the context of this section 'information' is data concerning a person's family, origin, connections, habits, proprietary rights and obligations, beliefs, health etc.[73] These criteria could be met if we say that the purpose of analysing network traffic was to find out the hacking habits of the attackers outside official criminal proceedings and without proper permission to conduct surveillance activities.

Based on the general theory of criminal law, to the extent that the purpose of analysing traffic data has to do with technical aspects of countering botnets and is not about collecting information about one specific intruder, the provision of unauthorised surveillance should not apply. However, whether § 137 could be a basis for holding persons performing unauthorised network surveillance accountable is to be determined by court practice.

Also, as mentioned above, the legal analysis may yield different results, depending on which person or authority is carrying out the surveillance. Here a distinction must be made whether this technique is used by the actual user of a computer connected to a botnet (e.g., private person, provider of a service) or by a third party (e.g., researcher, Computer Emergency Response Team – CERT, internet service provider – ISP). The main difference lies in the notion that listening to or recording the communication (regardless of whether it is encrypted or not)[74] by a party to the communication cannot be regarded as unauthorised surveillance in the meaning of criminal law. According to an Estonian Supreme Court's judgment, a person cannot wire-tap or record his own phone-call in a secret or concealed way, as the other party must take into account the possibility

[71] The translations of the Estonian legal acts into English are available on the website of the Estonian Ministry of Justice at http://www.just.ee/23295.

[72] *Sootak, J., Pikamäe, P.* Karistusseadustik. Kommenteeritud väljaanne. Juura, 2009, p. 405.

[73] *Ibid*, p. 406.

[74] The botmaster normally applies techniques to make the communication between the infected client and the C&C server not readable, e.g. by encryption.

that the communication be revealed.[75] The same principle applies irrespective of the communications channel used.

Additionally, if the packet inspection also encompasses the discovery of the content of the communication, it violates the right to confidentiality of communications as set forth in § 156 of the Estonian Penal Code.

> *§ 156. Violation of the confidentiality of a message*
> *(1) Violation of the confidentiality of a message communicated by a letter or other means of communication is punishable by a pecuniary punishment.*

A 'message' in the meaning of this section is only content data and not traffic data.[76] Therefore, if the content data of any message is not disclosed and provided that only traffic data is analysed, the referred section concerning violation of confidentiality does not apply.

German law lacks a provision comparable to § 137 of the Estonian Penal Code. The surveillance of a person by another private person is a crime if it reaches the level of stalking by e.g. establishing contact by any means of communication (§ 238(1) No. 2 of the German Penal Code). The provision penalising stalking does not show relevance in the context of packet and traffic data inspection, as such actions will surely not seriously infringe the freedom of action and/or of decision of the person affected, as required by the norm.[77] However, the surveillance of packet and traffic data can be punishable if it constitutes a violation of telecommunications secrecy[78] (§ 206 of the German Penal Code, § 88 of the Telecommunications Code, § 7(2) of the Telemedia Code), unlawful obtaining of data (§ 202a of the German Penal Code) or unlawful data interception (§ 202b of the German Penal Code).

The prohibition of the violation of the postal or telecommunications secrecy pursuant to § 206 of the German Penal Code applies to facts and information produced during the telecommunications or data transmission process.[79] The provision protects not only the facts[80] or the content of a telecommunication, but also the immediate circumstances of the telecommunication process (subpara. 5 sentence 2). Even the immediate circumstances of an unsuccessful attempt to make a connection are covered by the

[75] The Supreme Court of Estonia, Criminal Chamber ruling of 26 March 2009 no. 3-1-1-5-09.

[76] Although according to Estonian law, traffic data is not considered to be protected by the right to confidentiality of communications, it has to be noted that this may not be the case in other jurisdictions.

[77] *Eisele,* in: *Schönke/Schröder*, StGB, 28. Aufl., München, 2010, § 238, comment no. 4.

[78] *Unger*, Spam-Abwehr, DuD 2004, pp. 343; affirmative: *Tschope*, in: *Heidrich/Forgó/Feldmann* (Eds.), Heise Online Recht, 3. EL Oktober 2011, vol. 2, C. chapter III 4.4, comment no. 105.

[79] *Lenckner/Eisele,* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 6; *Fischer*, in: *Fischer*, StGB, 57. Aufl., München, 2010, § 206, comment no. 1; *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.), StGB, 3. Aufl., 2010, Vol. 2, § 206, comment no. 13.

[80] *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 7; in regard to the question which facts are covered by the telecommunications secret see: *Lenckner/Eisele* in *Sch/Sch* (*supra nota* 77), § 206, comment no. 6.

telecommunication secrecy (subpara. 5 sentence 3).[81] The 'immediate circumstances' of a communication process comprise, for example, end points of the communication, time of the internet session, method of the connection or its attempt, and are subject to the prohibition.[82] Importantly, IP addresses are covered by telecommunications secrecy as well.[83] As the inspection of packet and traffic data will include data referring to the telecommunication process between a C&C server and the bot(s), and thus the 'immediate circumstances' of a telecommunication process, the prohibition of the violation of the telecommunication process will be relevant in this context.

> *§ 206[84]. Violation of the postal and telecommunications secret*
> *(1) Whosoever unlawfully discloses to another person facts which are subject to the postal or telecommunications secret and which became known to him as the owner or employee of an enterprise in the business of providing postal or telecommunications services, shall be liable to imprisonment of not more than five years or a fine.*
> *(2) Whosoever, as an owner or employee of an enterprise indicated in subsection (1) above unlawfully*
> 1. *opens a piece of sealed mail which has been entrusted to such an enterprise for delivery or gains knowledge of its content without breaking the seal by using technical means;*
> 2. *suppresses a piece of mail entrusted to such an enterprise for delivery; or*
> 3. *permits or encourages one of the offences indicated in subsection (1) or in No 1 or 2 above, shall incur the same penalty.*
>
> *(3) Subsections (1) and (2) above shall apply to persons who*
> 1. *perform tasks of supervision over an enterprise indicated in subsection (1) above;*
> 2. *are entrusted by such an enterprise or with its authorization, to provide postal or telecommunications services; or*
> 3. *are entrusted with the establishment of facilities serving the operation of such an enterprise or with performing work thereon.*
>
> *(4) Whosoever unlawfully discloses to another person facts which became known to him as a public official outside the postal or telecommunications service on the basis of an authorised or unauthorised infringement of the postal or telecommunications secret shall be liable to imprisonment of not more than two years or a fine.*
> *(5) The immediate circumstances of the postal operations of particular persons as well as the content of pieces of mail are subject to the postal secret. The content of telecommunications and their immediate circumstances, especially the fact whether someone has participated in or is participating in a*

[81] *Ellinghaus*, in: *Arndt/Fezer/Scherer* (Eds.), TKG, Berlin, 2008, § 88, comment no. 13-17; *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 7.

[82] *Eisele* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 6; *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 7.

[83] Regional Court Hamburg, Decision of 23 June 2005, *LG Hamburg*, AZ 631 Qs 43/05, in: *Computerrecht* 2005, p. 832 seq, at p. 833; *Ellinghaus*, in: *Arndt/Fezer/Scherer* (supra nota 81), § 88, comment no. 15.

[84] German Codes quoted hereafter are official translations available on the website of the German Ministry of Justice (http://www.gesetze-im-internet.de/Teilliste_translations.html). Whenever such an official translation is not available, translation was provided by the authors of this report and is explicitly stated as such.

> *telecommunications event, are subject to the telecommunications secret. The telecommunications secret also extends to the immediate circumstances of unsuccessful attempts to make a connection.*

Thus, the crime of violating telecommunications secrecy is committed, if:

- an owner or employee of a professional communication service provider (ISP or company which provides communication services to its employees and allows the private use of the internet)
- a supervisor of such a company
- a sub-contractor providing telecommunications services, or
- a sub-contractor establishing facilities serving the operation of telecommunications services or performing work thereon
- a public official outside the postal or telecommunications service on the basis of an authorised or unauthorised infringement of the postal or telecommunications secrecy[85]

unlawfully discloses the facts of the immediate circumstances of the communication process to another person.[86] Thus, the mere saving of the telecommunications data in a protocol, without disclosing it to any other person, does not violate § 206.[87] However, an unlawful disclosure can be made even within the same company, if the person receiving the protected information does not need it according to the work structures, responsibilities and tasks related to providing the telecommunication service.[88]

Section 88 of the Telecommunications Code and § 7(2) of the Telemedia Code foresee compliance with 'telecommunications secrecy' as a legal obligation of electronic communications service providers. Interestingly, according to the definition of § 3 No. 6 lit. a and in accordance with No. 10 of the Telecommunications Code and § 2 No. 1 of the Telemedia Code, every company which allows private use of the company's internet devices by its employees is to be considered an ISP.[89] Telecommunication secrecy then refers also to the immediate circumstances such as end points of the communication or time of the internet session in regard to private internet use or also to business communications if they cannot clearly be separated from the private ones.[90]

[85] Referring to the different kind of offenders: *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 206, comment no. 19; *Fischer, in Fischer* (*supra nota* 79), § 206, comment no. 2.

[86] *Walter/Kargl, in: Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 206, comments no. 21-23; *Fischer, in Fischer* (*supra nota* 79), § 206, comments no. 6-9.

[87] *Schuster,* IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach §§ 202a, 206 StGB, in: ZIS 2/2010, p. 68-75, at p. 73.

[88] *Lenckner/Eisele* in *Sch/Sch* (*supra nota* 77), § 206, comments no. 10 and 36; Fischer, in Fischer (*supra nota* 79), § 206, comment no. 8.

[89] *Lenckner/Eisele* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 8.; *Braun, Telekommunikation am Arbeitsplatz, in: Heckmann* (Ed.), Internetrecht. JURIS Praxis Kommentar, 2. Aufl., Saarbrücken, 2009, p. 800, comments no. 97 and 103.

[90] *Braun,* Telekommunikation am Arbeitsplatz, in: *Heckmann* (Ed.) (*supra nota* 89), p. 800, comments no. 105-7.

> *§ 7. Telemedia Code. General Principles*[91]
> *(1) Telecommunication service providers are liable pursuant to applicable laws in regard to the information which they provide for use.*
> *(2) Telecommunication service providers pursuant to §§ 8 to 10 are neither obliged to monitor the data they process or store nor to search for circumstances which would indicate an illegal activity. The obligation to remove or block the use of information pursuant to the laws remain unaffected even in the case of lack of liability of a telecommunication service provider pursuant to §§ 8 to 10. The secrecy of telecommunications pursuant to § 88 of the Telecommunications Code is to be observed.*
>
> *§ 88. Telecommunications Code. Privacy of Telecommunications*
> *(1) The content and detailed circumstances of telecommunications, in particular the fact of whether or not a person is or was engaged in a telecommunications activity, shall be subject to telecommunications privacy. Privacy shall also cover the detailed circumstances surrounding unsuccessful call attempts.*
> *(2) Every service provider shall be obliged to maintain telecommunications privacy. The obligation to maintain privacy also applies after the end of the activity through which such commitment arose.*
> *(3) All persons with obligations according to subsection (2) shall be prohibited from procuring, for themselves or for other parties, any information regarding the content or detailed circumstances of telecommunications beyond that which is necessary for the commercial provision of their telecommunications services, including the protection of their technical systems. Knowledge of facts which are subject to telecommunications privacy may be used solely for the purpose referred to in sentence 1. Use of such knowledge for other purposes, in particular, passing it on to other parties, shall be permitted only insofar as provided for by this Act or any other legal provision and reference is made expressly to telecommunications activities. The reporting requirement according to section 138 of the Penal Code shall have priority.*

The secrecy of telecommunications, as set forth in § 7(2) of the Telemedia Code and in § 88(3) of the Telecommunications Code, includes the prohibition of disclosure of the protected data to others, e.g. a private researcher, or even to other persons working within the facility providing the communication service (other than for purposes of invoicing). It is noteworthy that, according to the Administrative Court of Hessen, the secrecy of telecommunications applies only during the telecommunications process; after the end of the telecommunications process the saved data will be protected by provisions of data privacy.[92]

However, according to § 88(3) of the Telecommunications Code the prohibition to disclose protected data to others does not expressively apply to information which is

[91] Translation by Dr. Katharina Ziolkowski.
[92] See *VGH Kassel*, judgment of 19. May 2009, file no. 6 A 2672/08. Available at http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=VGH%20Hessen&Datum=19.05.2009&Aktenzeichen=6%20A%202672/08. See also: *BVerfGE* 115, p. 166, 184; *Ellinghaus*, in: *Arnt/Fezer/Scherer* (fn 83), § 88, comment no. 20.

necessary for either providing the services or for the protection of their own technical systems. Accordingly, § 100 of the Telecommunications Code allows a communication service provider to collect and use customer and traffic data in order to recognise, limit or eliminate a disturbance or error of the telecommunication systems. Bearing in mind the principle of the 'unity of the law system', the provision is relevant for the assessment of the criterion of 'unlawfulness' of data disclosure as required by § 206(1) of the German Penal Code.[93] Therefore, when § 100 of the German Telecommunications Code is applicable, data processing for the purposes stated above (to recognise, limit or eliminate a disturbance or error of the telecommunication systems) does not lead to a violation of postal and telecommunications secrecy (§ 206 of the German Penal Code, § 88 of the German Telecommunications Code). A disturbance or error in the telecommunication system could be caused, for example, when a botnet is used for DDoS attacks.[94]

> *§ 100. Faults in Telecommunications Systems and Telecommunications Service Fraud*
> *(1) Where required, the service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems.*
> *(2) For purposes of changed implementations and the identification and location of faults in the network, the operator of the telecommunications system and his authorised representative shall be allowed to break in on existing connections, as far as this is operationally required. Break in shall be indicated by means of an acoustic signal and explicitly notified to the parties concerned.*
> *(3) Where required, the service provider may collect and use the customer data and traffic data needed to detect and put a stop to the surreptitious use of services and other unlawful use of telecommunications networks and services when there are grounds, to be recorded in writing, to suppose such use. For the purpose referred to in sentence 1 the service provider may use collected traffic data in such a way as to identify, from the total traffic data not more than six months old, the data relating to those network connections in respect of which there are grounds to suppose that unlawful use of telecommunications networks and services has been made. In particular, the service provider may set up a pseudonymised data file from the customer data and the traffic data collected under sentence 1 which provides information on the revenues generated by the individual subscribers and which, suitable fraud criteria being applied, allows network connections in respect of which there are grounds to suppose that surreptitious use of services has been made, to be found. Data relating to all other communications are to be erased without undue delay. The Regulatory Authority and the Federal Data Protection Commissioner are to be notified without undue delay of the introduction of, and any modification to, the procedure according to sentence 1.*
> *(4) Subject to the conditions referred to in subsection (3) sentence 1 the service provider may, in a given instance, collect and use control signals to*

[93] See: *Lenckner/Eisele* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 13; *Fischer*, in *Fischer* (*supra nota* 79), § 206, comment no. 9; . *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 206, comment no. 44.

[94] *BGH,* Urt. v. 13.01.2011, III ZR 146/10, comment no. 8.

> *the extent that this is indispensable to clarify and put a stop to the acts specified there. Collection and use of any other communications content is not permitted. The Regulatory Authority is to be notified of measures according to sentence 1 taken in a given instance. The parties concerned are to be advised as soon as it is possible to do so without the purpose of the measures being compromised.*

According to a decision by the German Federal Supreme Court in 2011, § 100(1) of the Telecommunications Code allows ISPs to collect and analyse users' IP addresses for up to seven days on a general basis, i.e. without any concrete findings, in order to detect, locate and eliminate faults and malfunctions in its network and telecommunication systems.[95] The court decision underlines that the sending of spam, the dissemination of malicious software (trojan horses, viruses etc.) and the misuse of computer systems for running DDoS can cause significant faults and malfunctions in telecommunication systems.[96] Therefore, the collection and processing of traffic data (including IP addresses) for the purposes of detecting and eliminating sources of spam-sending, DDoS operations and thus also botnets is covered by the permission granted under § 100(1) of the Telecommunications Act. Once findings and concrete reasons for faults and malfunctions have been detected within the period of seven days, the ISP is allowed to save and analyse the appropriate data for a period longer than seven days, namely as long as the data is needed to eliminate the reasons for the fault or the malfunction.[97]

The mere surveillance of packet and traffic data by an ISP or a CERT of a company will mostly not violate the prohibition of unlawful obtaining of data according to § 202a of the German Penal Code, as the provision refers to data which are 'especially protected against unauthorised access'. Judicial practice and scholarly writings consider a special protection to be given in the case of encryption (during the data transmission process), password protection, magnetic cards, biometric sensors and the like (in contrast to, e.g., mere saving of data under a misleading file name or under a misleading folder name or saving contents in a seldom-spoken language).[98] Thus, surveillance of packet and traffic data will only fall under the crime of 'data espionage' if the packet and traffic data were protected against unauthorised access, e.g. by encryption or by a password. A penalty could be possible if, for example, a researcher hacked into the computer system of an ISP in order to gain packets and traffic data, in a case where the penetrated system was password-protected.

> *§ 202a. Data espionage*
> *(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if*

[95] *BGH,* Urt. v. 13.01.2011, III ZR 146/10 comments no. 3, 6.

[96] *BGH,* Urt. v. 13.01.2011, III ZR 146/10, comment no. 8.

[97] The German Federal Supreme Court explicitly names a period of some days, in which the provider must be given the possibility to react on incoming information about faults and malfunctions (*BGH,* Urt. v. 13.01.2011, III ZR 146/10, comment no. 8.). Therefore the period of time is strictly limited to a small number of days, maybe weeks.

[98] *Lenckner/Eisele* in *Sch/Sch* (*supra nota* 77), § 206, comment no. 8; *Fischer*, in: *Fischer* (*supra nota* 79), § 202a, comment no. 9a; *Leckner/Winkelbauer*, CR 1986, p. 487.

> *he has circumvented the protection, shall be liable to imprisonment of not more than three years or a fine.*
> *(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.*

However, surveillance of packet and traffic data which are not especially protected against unauthorised access can be punishable as unlawful data interception according to § 202b of the German Penal Code, a norm which is subsidiary to the aforementioned § 202a.[99]

> *§ 202b. Data Interception*
> *Whosoever unlawfully intercepts data (§ 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment of not more than two years or a fine, unless the offence incurs a more severe penalty under other provisions.*

The interest which the norm aims to protect is the 'formal interest' of the authorised person in the confidentiality of a communications process, which does not have to meet the subjective interest of the persons involved.[100] Communication data of past and completed transmission processes is not protected by the norm.[101] This means that the aim of the provision is to criminalise unauthorised 'sniffing' of unprotected networks in regard to non-public data processing. The requirement of 'non-public' data processing refers to all communication data during the transmission process in the context of emails, internet chats, VPN-connections or VoIP.[102] Interception of such data, if not 'intended' for the intercepting person, is punishable, in contrast to communication data of 'public' data processing, i.e. all data aimed for the general public. The lack of encryption of the data transmitting process does not mean that the data is meant to be available to the general public.[103] Of course, data interception by owners or employees of an ISP, as far as necessary for the conduct of the service, will not violate the prohibition, as such data is 'intended' for the persons involved in providing the service.

Thus, owners and employees of ISPs or CERTs of companies can only conduct *ad hoc* packet and traffic data inspection and analysis in order to detect and characterise a botnet without committing a crime, insofar as it is necessary to recognise, limit or eliminate a disturbance or error of their own telecommunications systems. Such situations are imaginable in cases of botnet activities creating major spam traffic or uses of the

[99] *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 10; *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 202b, comment no. 11.

[100] *Eisele* in *Sch/Sch* (*supra nota* 77), § 202b, comment no. 1; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 2.

[101] *Eisele* in *Sch/Sch* (*supra nota* 77), § 202b, comment no. 3; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 3.

[102] *Eisele* in: *Sch/Sch* (*supra nota* 77), § 202b, comment no. 3; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 4.

[103] *Eisele* in: *Sch/Sch* (*supra nota* 77), § 202b, comment no. 4.; *Fischer*, in: *Fischer* (*supra nota* 79), § 202b, comment no. 3.

customers' computers for DDoS attacks. Corresponding to the aforementioned aim of the data inspection for purposes of elimination of a disturbance or error of their own telecommunication systems, the data would have to be deleted immediately after the elimination of the disturbance or error. They could definitely not be passed to an independent researcher without being anonymised, as this would constitute the crime of violation of telecommunications secrecy. An independent researcher monitoring packet and traffic data is risking committing a forbidden 'interception of data' if collecting data on internet sessions which are 'non-public' in the meaning of the respective provision.

In all cases of packet and traffic data surveillance, the consent of the communication participant whose data were collected and/or stored eliminates the criminal liability of the persons conducting the surveillance. However, it should be mentioned that, based on considerations in regard to customer protection, the law sets very definite and sophisticated criteria for the consent of a client for the collection and storage of his data by the communications service providers and, at the same time, obliges the service providers to give in advance detailed information about the kind of data to be collected and stored as well as the aim of the collection and storage. The consent to packet and traffic data surveillance becomes relevant in the context of § 206 of the German Penal Code only if given by all persons participating in the telecommunications process.[104] In most cases, this condition will be not given in regard to the telecommunications partner who controls the botnet and thus establishes a telecommunication process between the C&C instance and the computer part of the botnet. In the case of packet and traffic data monitoring within a company, the implementation of such a monitoring would be considered a 'technical monitoring measure' which would require the consent of the works council, if existing (see § 87 para. 1 No. 6 Works Council Constitution Code).

Further, the surveillance and disclosure of packet and traffic data will not be punishable if it occurs on the basis of a court order, in the context of authorised law enforcement or other state agency investigations foreseen by the law as in § 100a of the German Code of Criminal Procedure or in the context of danger prevention measures by police authorities according to the 16 different police codes of the German States[105] or § 20k of the Code on the Federal Criminal Police Office. For investigating activities and other proceedings by the law enforcement agencies, there should be a concrete suspicion of someone having committed a criminal act.

All in all, it can be asserted that 'investigations' in regard to botnets, which include collecting data about the 'immediate circumstances' of a telecommunications process, are primarily within the responsibility of law enforcement authorities. Correspondingly, pursuant to § 7(2) of the Telemedia Code telecommunications service providers do not have the responsibility to monitor the processed or stored information or to research for

[104] *BVerfGE* 85, p. 399; *Sachs*, JuS 1992, p. 960; *Lisken*, NJW 1994, p. 2069; *Dann/Gastell*, NJW 2008, p. 2946; *Lenckner/Eisele* in: *Sch/Sch* (*supra nota* 77), § 206, comment no. 12; *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 206, comment no. 45.

[105] See: *Eisele*, in: *Sch/Sch* (*supra nota* 77), § 238, comment no. 13; interestingly, the Federal Police is not responsible for the prosecution of crimes in regard to telecommunication, which often will cross the border of different federal states, see art. 12 of the Federal Police Code. Available at http://www.gesetze-im-internet.de/bgsg_1994/__12.html.

information which could indicate illegal activities.[106] This includes research for unknown risks.[107] However, if knowledge of an illegal activity is given, claims of cease and desist, even as a preventative measure, can arise.[108] Any private person monitoring packet and traffic data – for reasons other than what are necessary to operate a telecommunications service or to eliminate disturbances or errors thereof – has to obey the penal and other laws protecting the secrecy of the telecommunications process. Thus, only a search for or research of a botnet by using anonymised data, i.e. excluding IP addresses and other data protected by telecommunications secrecy, which is obtained in a lawful way, would be acceptable in regard to penal law provisions.

Privacy Concern – Data Protection

In some jurisdictions, especially in countries implementing the EU Data Protection Directive,[109] IP addresses may be considered personal data[110] and are therefore subject to personal data processing requirements, including the principle of legality *(personal data shall be collected only in an honest and legal manner)* and the principle of purposefulness *(personal data shall be collected only for the achievement of determined and lawful objectives, and they shall not be processed in a manner not conforming to the objectives of data processing).*[111]

Since the issue of considering IP addresses as personal data can be and is debated, but the discussion itself is beyond the scope of this report, a position on whether IP addresses

[106] The details of the responsibilities of a telecommunication service provider are subject to debates within the scholarly writings and jurisdiction, see: *Heckmann*, chapter 1.7 - § 7 Telemediengesetz, in: *Heckmann (*Ed.*)* (*supra nota* 89), comments no. 132 seq.

[107] *Ibid.*, comment no. 134.

[108] *Ibid.*, comments no. 70-108.

[109] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995, P. 0031 – 0050.

[110] According to Article 2(a) of the Data Protection Directive 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[111] According to § 6 of the Estonian Personal Protection Act on processing of personal data, a processor of personal data is required to adhere to the following principles:

1) principle of legality – personal data shall be collected only in an honest and legal manner;
2) principle of purposefulness – personal data shall be collected only for the achievement of determined and lawful objectives, and they shall not be processed in a manner not conforming to the objectives of data processing;
3) principle of minimalism – personal data shall be collected only to the extent necessary for the achievement of determined purposes;
4) principle of restricted use – personal data shall be used for other purposes only with the consent of the data subject or with the permission of the competent authority;
5) principle of high quality of data – personal data shall be up-to-date, complete and necessary for the achievement of the purpose of data processing;
6) principle of security – security measures shall be applied in order to protect personal data from involuntary or unauthorised processing, disclosure or destruction;
7) principle of individual participation – the data subject shall be notified of data collected concerning him or her, the data subject shall be granted access to the data concerning him or her and the data subject has the right to demand the correction of inaccurate or misleading data.

should be regarded as personal data or not is not taken here. However, if IP addresses were considered personal data, the stakeholder capturing and analysing the traffic would, under § 10 of the Estonian Personal Data Protection Act,[112] need the consent of the data subject.[113]

> *§ 10. Permission for processing personal data*
> *(1) Processing of personal data is permitted only with the consent of the data subject unless otherwise provided by law.*

The cases when the processing of personal data is allowed without the data subject's consent are comprehensively listed in § 14 of the Personal Data Protection Act.

> *§ 14. Processing of personal data without consent of data subject*
> *(1) Processing of personal data is permitted without the consent of a data subject if the personal data are to be processed:*
> *1) on the basis of law;*
> *2) for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;*
> *3) in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible;*
> *4) for performance of a contract entered into with the data subject or for ensuring the performance of such contract unless the data to be processed are sensitive personal data.*

Taking into account § 14, an example of a situation in which the data subject's consent is not required is an ongoing criminal proceeding, where the authority of law enforcement overrides the requirement of consent; also, exceptions to the consent requirement might arise from other legal obligations related to national security and public order.

According to § 5 of the Personal Data Protection Act, processing of personal data is *"any act performed with personal data, including the collection, recording, organization, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage, combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used".*[114]

A situation where the packet and traffic records include personal data and are captured and analysed by a person who has not acquired the data subject's consent, such as a researcher, creates a basis for invoking administrative liability. Becoming aware of such conduct, the data subject may apply to the Data Protection Inspectorate or to a court according to § 22 of the Personal Data Protection Act claiming that his rights have been violated. From the practical side, the question of which parties to the communication (the

[112] Personal Data Protection Act. 15 February 2007. – RT I 2007, 24, 127; RT I, 30.12.2010, 2.
[113] A data subject is a person whose personal data are processed – § 8 of Personal Data Protection Act.
[114] *Supra nota* 112.

bot owner or the botmaster) might be interested in filing such a complaint arises. The probability of the botmaster initiating any official proceedings is relatively low (although should not be eliminated), leaving the user of the infected computer in the botnet the more likely party to file a complaint. In practical terms, such a possibility should be considered rather theoretical, since the owner of an infected computer is not expected to turn against a researcher acting in good faith.

> *§ 22. Data subject's right of recourse to Data Protection Inspectorate or court*
> *A data subject has a right of recourse to the Data Protection Inspectorate or a court if the data subject finds that his or her rights are violated in the processing of personal data, unless a different procedure for contestation is provided by law.*

The fact that packets from malevolent users may be monitored does not alter the legal assessment, because in accordance with the rule of law all internet users have their right to privacy. This means that malevolent users are not deprived of their right to privacy even when they commit wrongful acts such as botnet attacks. Their privacy right may be invaded without their consent only by competent authorities, such as the police investigating a botnet attack.

To eliminate legal risks related to monitoring and analysing traffic from an ISP's point of view, consent from the data subjects needs to be obtained. This can be done by including respective provisions in service level and user agreements and also in the terms of use of its information services and networks. The theoretical risk of a complaint being filed by the botherder still remains, which can be minimised by monitoring and analysing traffic on an abstract level and by anonymising personal data. It must be noted that the justification for traffic monitoring and analysis in case the consent is received is limited to the customers of one certain ISP. Inspecting traffic data is less problematic in cases where specific exceptions and authority exceeding data protection restrictions have been provided for by law.

The German data protection law is enshrined in the Federal Data Protection Code and in sixteen Data Protection Codes of the States. The former applies to all federal government entities (and in certain cases to state government entities) as well as to non-state entities. The different Data Protection Codes of the sixteen states bind all state government entities, including municipalities and other local authorities. The laws provide a wide spectrum of protection, e.g. the right of the data subject to information and to correct, delete or seal data; possibilities to file a complaint or sue a public authority or company *inter alia* for damages; the establishment of data protection ombudsmen at federal and state level; the obligation to appoint data protection administrators in companies employing at least twenty persons.

Further, specific data protection regulations can be found in countless other codes, e.g. in §§ 91-107 of the Telecommunication Code and §§ 11-15a of the Telemedia Code. Although those special laws always have priority, especially in regard to circumstances during a telecommunications process, the provisions of general laws apply considering the 'unity of law'.

The definition of personal data is set forth in the Federal Data Protection Code:

> *§ 3. Further definition*
> *'Personal data' means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).*

As mentioned above, a detailed discussion on whether IP addresses are to be deemed personal data will be omitted in the present survey. However, it shall be only mentioned that some controversy is also to be found within the German scholarly writings and judicial practice.[115] However, as a general observation it can be asserted that, according to German law, even dynamic IP addresses should be considered as personal data.[116]

In regard to data collection, processing and use, § 4 of the Federal Data Protection Code, like the special provisions of § 91 seq. of the Telecommunications Code and § 12(1) of the Telemedia Code, state a general prohibition.

> *§ 4. Admissibility of Data Collection, Processing and Use*
> *The collecting, processing and use of personal data shall be admissible only if this Act or any other legal provision permits or prescribes them or if the data subject has consented.*

In this context, it is especially important to consider that according to § 15(1) of the Telemedia Code, a service provider is allowed to collect the personal data of its customers only as far as it is necessary for providing or billing for the service.

> *§ 15. Telemedia Code: Data on usage*[117]
> *(1) The service provider may collect and use the personal data of a recipient of a service, only to the extent necessary to enable and bill for the use of telemedia (data on usage). Data on usage are in particular:*
> 1. *characteristics to identify the recipient of the service,*
> 2. *information about the beginning, the end and the duration of each use, and*
> 3. *information about the telemedia used by the recipient of the service.*

[115] See, e.g., *OLG Hamburg*, Beschl. v. 03.11.2010 – 5 W 126/10; *LG Wuppertal*, Beschl. v. 19.10.2012 – 25 Qs 10 Js 1977/08 – 177/10, 25 Qs 177/10; *AG München*, Urt. v. 30.09.2008 – 133 C 5677/08; *AG Berlin-Mitte*, Urt. v. 27.03.2007 – 5 C 314/06; *VG Wiesbaden*, Beschl. v. 27.02.2009 – 6 K 1045/08.WI; *Arning/Forgó/Krügel*, DuD 2006, p. 704; *Ernst/Spoenle*, CR 2007, p. 439; *Pahlen-Brandt*, DuD 2008, p. 37; *Bär*, MMR 2008, p. 632; *Pahlen-Brandt*, K&R 2008, p. 288; *Meyerdierks*, MMR 2009, p. 8; *Weichert*, VuR 2009, p. 323; *Kirchberg-Lennartz/Weber*, DuD 2010, p. 479; *Heidrich/Wegener*, DuD 2010, p. 172; *Sachs*, CR 2010, p. 547; *Nietsch*, CR 2011, p. 763; *Freund/Schnabel*, MMR 2011, p. 495; *Eckhardt*, CR 2011, p. 339; *Wegener/Heidrich*, CR 2011,pp. 479.

[116] See: *AG Berlin-Mitte*, Urt. v. 27.03.2007 – 5 C 314/06; *VG Wiesbaden*, Beschl. v. 27.02.2009 – 6 K 1045/08.WI; *Pahlen-Brandt*, DuD 2008, p. 37; *Pahlen-Brandt*, K&R 2008, p. 288; *Weichert*, VuR 2009, p. 323; *Wegener/Heidrich*, CR 2011, p. 479.

[117] Translation by Dr. Sebastian Brüggemann.

In the case of packet and traffic data collection by a CERT or IT-security personnel within a company, including personal data, § 32 of the Federal Data Protection Code becomes relevant. The norm aims to protect employees against ‘covered monitoring’.[118]

> *§ 32. Federal Data Protection Code: Data Collection, Processing and Use for Employment-Related Purposes*
> *(1) An employee’s personal data may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees’ personal data may be collected, processed or used to investigate crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime, and the employee does not have an overriding legitimate interest in ruling out the possibility of collection, processing or use, and in particular the type and extent are not disproportionate to the reason.*
> *(2) Subsection 1 shall also apply when personal data are collected, processed or used without the help of automated processing systems, or are processed or used in or from a non-automated filing system or collected in such a filing system for processing or use.*
> *(3) The rights of participation of employee staff councils shall remain unaffected.*

According to this provision, collecting, processing and use of communication data is only allowed in order to investigate crimes. Within scholarly writings, the provision is widely criticised for not stating an authorisation for preventive monitoring of employees’ communications, including data on the ‘immediate circumstances’ of a communication process, such as end points of the communication, time of the internet session, method of the connection or its attempt.[119] Partly, control of the immediate circumstances of a telecommunication process is considered legal in cases where private use of the internet is forbidden and the employer aims to enforce the internal regulation.[120]

At the same time, the Federal Data Protection Code provides some exceptions. In regard to storage, modification and use of personal data by private entities, § 28 states the following:

> *§ 28. Federal Data Protection Code: Collection and Storage of Data for Own Business Purposes*
> *(1) The collection, storage, modification or disclosure of personal data or their use as a means of fulfilling one's own business purposes shall be admissible*
> 1. *[…]*
> 2. *insofar as this is necessary to safeguard justified interests of the data controller and there is no reason to assume that the data subject has*

[118] *Braun,* Telekommunikation am Arbeitsplatz, in: *Heckmann (Ed.)* (*supra nota* 89), p. 800, comment no. 70.
[119] *Ibid*., comments no. 71, 82, 85, 86, 93 with further references.
[120] *Ibid*., comments no. 93-95.

> *an overriding legitimate interest in his data being excluded from processing or use,*
>
> *3. […]*
>
> *4. […]*
>
> *During the process of collecting the data the purpose of the data processing or use shall be identified in detail.*
>
> *(2) Communication or use shall also be admissible*
>
> 1. *[…]*
> 2. *as far as necessary*
>   *a. to safeguard the interests of a third party*
>   *b. […] and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from disclosure of use.*
> 3. *if it is necessary for a research entity in order to conduct a scientific research, the scientific interest to conduct the research project substantially predominates over the interest of the data subject in exclusion of the change of purpose the data was collected for, and if the research cannot be conducted otherwise or can otherwise be conducted under disproportional effort.*
>
> *(3) – (9) […]*

The provision shows that personal data protection is by no means absolute. It allows the collection, storage, modification, disclosure or use of personal data, if the interest of the data controller or a third party overrides the interest of the data subject in his data being excluded from the above actions.[121] In regard to the surveillance of package and traffic data in order to detect and characterise a botnet, it is doubtful whether this could be defined as a legitimate interest of an ISP or CERT of a company. According to the mission of an ISP or CERT, they should only have a predominant interest in personal data if knowledge about the personal data is necessary to enable and maintain the concrete telecommunications process or to eliminate disturbances or errors of their own telecommunications system. The above assessment is confirmed by the special data protection regulations provided by the Telemedia Code and Telecommunications Code. According to § 9 of the Telemedia Code, communication service providers are allowed to automatically store data for a short period of time in order to conduct or improve the efficiency of the communication services, but not for other reasons. Pursuant to § 100 of the Telecommunications Code, communication service providers may collect and use customer and traffic data in order to recognise, limit or eliminate a disturbance or error of their own telecommunication systems.

In summary, there is a difference in the competences of the ISPs (i.e. access providers) which have the authority to save the IP addresses up to seven days according to § 100 I of the Telecommunication Code on the one hand and the operators of websites on the other hand. Due to the provisions of the German Telemedia Law, the operators of websites may only store the data for the purpose of the service itself but not for the reasons stated in § 100 of the Telecommunications Code; the Telemedia Code does not include a provision comparable to § 100 of the Telecommunications Code. This leads to a lack of

[121] *Gola/Schomerus*, in: *Gola/Schomerus* (Eds.), BDSG, 11. Aufl., München, 2012, § 28, comments no. 24-30.

synchronisation in the legal framework regarding the competences of operators of internet services (i.e. operators of websites), who do not act under the provisions of the Telecommunications Code.

However, according to § 93 of the Telecommunications code and § 13 of the Telemedia Code, ISPs do have the responsibility to inform the customer, when concluding contracts, of the nature, extent, place and purpose of the collection and use of personal data in such a way that the subscribers are given notice, in readily comprehensible form, of the basic data processing facts.

A private researcher of a botnet would have to prove that the use of personal data, which were already collected by someone else in a lawful way, does meet the test of § 28(2) No.3 of the Federal Data Protection Code, in order not to violate data protection rules (necessity to use data; 'substantial predominance' of the scientific interest over the interest of the data subject in exclusion of the change of purpose the data was collected for; the research cannot be conducted otherwise or can otherwise be conducted with disproportional effort only).[122]

As studying a botnet may be seen as a kind of private investigation in criminal matters, it should be underlined that the storage of communication data for up to six months for *inter alia* law enforcement purposes (not related to an individual case or current investigation) as envisioned by § 113a and b of the Telecommunication Code was found to be void by the German Constitutional Court in 2010.[123]

Again, also in regard to data protection laws, consent of the data subject excludes the illegality of collecting, processing, using or disclosing personal data. Also in this context, German laws provide sophisticated requirements for the consent to be legally relevant,[124] and, at the same time, oblige the entity collecting, storing and using the data to provide in advance detailed information about the aim of the collection, storage and use (see §§ 4, 4a of the Federal Data Protection Code).[125] In the context of surveillance of internet communications within a company (in which the private use of the internet is not forbidden), the consent must be provided individually – it is not sufficient to state a consent within a company or bargaining agreement.[126]

Of course, the surveillance and disclosure of package and traffic data will not violate data protection if it occurs on the basis of a court order, in the context of lawful law enforcement investigations or danger prevention measures by police authorities (see § 14 (2) Telemedia Code and §§ 112, 113 Telecommunication Code). The illegality in regard to the data protection regulations is also excluded if the surveillance of package and traffic data in order to detect and characterise a botnet is conducted by using anonymised

[122] *Gola/Schomerus*, in: *Gola/Schomerus* (Eds.) (*supra nota* 121), § 28, comments no. 14-23, 24-30.

[123] Federal constitutional Court, Decision of 2 March 2010, *BVerfG,* Urt. v. 02.03.2010, I 272 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 .

[124] *Gola/Schomerus*, in: *Gola/Schomerus* (Eds.) (*supra nota* 121), § 4, comments no. 15-16, § 4a, comments no. 19-32, 34-35.

[125] *Ibid*., § 4, comments no. 29-31.

[126] *Ibid*., 124., § 4a, comment no. 21.

data. In that case the data no longer relates to a certain person, and therefore the data protection regulations do not apply.

A violation of data protection provisions can result in a monetary fine (§ 43 Data Protection Code) or even amount to a criminal offence (§ 44 Data Protection Code).

Honeypots

"[A] honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."[127] Honeypots provide 'fake' services like databases, file servers, web servers or client computers, which run on common operating systems, but as a unique characteristic, they are intentionally designed to be vulnerable to attacks. The purpose of the vulnerabilities is to attract malevolent network traffic[128] in order to monitor and log exploitation attempts. The person running the honeypot gets easy access to all traffic as well as content data of any communication accessing the honeypot. In the context of botnets, this includes receiving a sample of botnet malware after a successful exploitation, which is usually forwarded to anti-virus companies for further analysis. To a limited extent, honeypots can also be used to study the spreading mechanism of a botnet or the communication behaviour of a bot.

Although a honeypot is another technical tool to monitor and study network traffic, from a legal perspective it presents a few unique characteristics. More precisely, the person using a honeypot might claim that he is not violating the confidentiality of messages as set forth in § 156 of the Estonian Penal Code (discussed above) because he is a party to the communication. This argument is based on the fact that the offence can only be committed by a person for whom the message was not intended.[129] In the context of botnet attacks, the owner of the botnet started the communication and directed it, among other targets, also at the honeypot. Having said this, the owner of the honeypot can claim that the communication should be considered as intended, among others, also for him.

However, when assessing the legality of actions undertaken with the use of honeypots, the presence of a third party should not be forgotten. The possibility that the traffic in the honeypot might not only contain messages from the botmaster but also from other users,

[127] Know Your Enemy. Learning About Security Threats. Second Edition. The Honeynet Project. Addison-Wesley 2004, p. 18.

[128] Despite the fact that most literature available on honeypots claims the opposite, saying that honeypots are not advertised anywhere and they do not attract any traffic, this statement seems to have derived from discussions on the legal acceptability of using this technology. The term itself, honeypot, suggests that just like a honeypot draws bees, an infotechnological honeypot is set up so that due to its vulnerabilities it is attractive to hackers. See contrary opinions: Comments on the Aftenposten article. Norwegian Honeynet Project, 2 July 2009. Available at: http://www.honeynor.no/2009/07/02/comments-on-the-aftenposten-article/; Know Your Enemy: Honeynets, 31 May 2006. Available at: http://old.honeynet.org/papers/honeynet/.

[129] *Sootak, J., Pikamäe, P.* Karistusseadustik. Kommenteeritud väljaanne (*supra nota* 72), p. 441.

including bot owners whose computers have been ordered to spread traffic, has to be taken into account. By monitoring such traffic, the owner of the honeypot still risks violating the confidentiality of communications – an activity not falling under the principle explained above, according to which a person is not committing the offence if the traffic is intended for him.

The second potential privacy concern, in addition to respecting the confidentiality of communications, relates to personal data processing. Naturally, if the employment of a honeypot results in the processing of personal data, the respective data protection requirements, as also discussed above, would have to be followed.

According to German law, during the telecommunication process the traffic data between a botmaster or a bot on the one side and the honeypot of a telecommunications service provider on the other side can be legally monitored by the latter only as far as this is necessary to enable and maintain the individual telecommunication process or in order to recognise, limit or eliminate a disturbance of the telecommunication systems (see discussion above). Otherwise it violates the 'telecommunications secrecy' pursuant to § 206 of the German Penal Code as well as the legal obligations according to § 88 of the Telecommunications Code and § 7(2) of the Telemedia Code and data protection laws. As stated before, only certain botnet activities would indeed constitute a disturbance to providing services and thus only these can be seen as a legitimate reason for the surveillance of packet and traffic data within a honeypot.

Disclosure of the data gained as a result of the surveillance, e.g. to an independent researcher, is only allowed with the consent of the communication participants, after the anonymisation of the data, or if it occurs on the basis of a court order, in the context of lawful law enforcement investigations or danger prevention measures by police authorities (see § 14(2) Telemedia Code and §§ 112, 113 Telecommunication Code).

A private researcher using a honeypot to monitor traffic is not violating telecommunications secrecy as he is a participant in the individual telecommunication process between a botmaster or bot on the one side and him, via his honeypot, on the other side. As the traffic data received within the honeypot are 'intended' for him as the participant of the telecommunication process, the penalty for an unlawful interception of data according to § 202b of the German Penal Code will not be imposed. Also, as far as a private researcher analyses data which are not 'especially protected against unauthorised access', § 202b of the German Penal Code ('data espionage') will not apply. However, a private researcher would have to prove that the collection, storage and use of personal data, which he collects by analysing the honeypot, is necessary to safeguard his justified interests and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use (§ 28(1) No. 2) of the Federal Data Protection Code). In most cases, it will be a major challenge to provide such a proof. It should be underlined that the possibility the law provides to collect, store and use data for 'scientific interests' refers to data which were collected by someone else in a lawful way (see § 28(2) No. 3 of the Federal Data Protection Code).

Takedown of Command and Control Servers

An essential part of every botnet is the C&C server (or C&C infrastructure), as without it the bots would not receive any new commands and would largely remain inactive, except for frequently trying to establish contact with the C&C server. Because of their critical role, C&C servers have become a prime target for botnet takedown attempts, in reaction to which botnet developers have invented different C&C server topologies in an effort to mitigate the risk of a C&C server takedown. The most common topologies are to have one C&C server or a small network of them distributed globally.

A takedown of this type of botnet can be achieved by: a) disconnecting the identified C&C server(s) by deleting its DNS name; b) making the C&C server(s) unavailable by black-holing the traffic directed to it; c) physically seizing the C&C server(s); d) disconnecting the C&C server(s) by the ISP or the cloud service provider hosting it.

Using authorised force to take down a C&C server

The legal aspects of taking down C&C servers depend on the authorities ordering and implementing the takedown and on the location of the C&C servers. For example, if a C&C server is located in Estonia, the Estonian Computer Emergency Response Team (CERT-EE)[130] would normally contact the relevant ISP and ask it to disconnect the server. Should the server be based abroad, CERT-EE would either contact the foreign ISP or the national CERT of the respective state.

From a legal perspective, according to Estonian legislation, CERTs normally do not have the authority to order a C&C server takedown. An ISP can decide to restrict access to certain resources in accordance with its general security mandate (see section below on Duty to Act against Botnet Attacks: Internet Service Providers) with possible limitations arising from consumer protection, user agreements etc. In case of a request by a law enforcement authority (the police, courts) the service provider is obliged to restrict access to its services.

There are different legal constructs for the police to order takedown. If the botnet attacks pose a danger to or violate the public order, the police can, according to the Police and Border Guard Act[131], request the person disturbing public order to remove the danger or eliminate the violation. In terms of a botnet attack the person in question could, in addition to the person in charge of the C&C server, also be the botmaster as well as the owner of a certain bot. However, giving this order to all individual bot owners is in the majority of cases not feasible, since it could mean thousands of people whose computers are part of a particular botnet.

[130] CERT-EE is an organisation responsible for the management of security incidents in '.ee' computer networks. CERT-EE is also the national point of contact for international cooperation in the field of IT security. See: http://www.cert.ee.

[131] Police and Border Guard Act. 6 May 2009. – RT I 2009, 26, 159; RT I, 04.07.2012, 1.

> *§ 7^{13}. Control action and application of administrative coercive measure*
> *(1) In case of danger to or violation of public order the police has the right to oblige the person responsible for public order to remove the danger or eliminate the violation of public order and notify the person of the application of administrative coercive measures pursuant to subsection 2 or 3 of this section if the person does not perform the duty within the term set in the notification.*

The Police and Border Guard Act provides for a very general definition of the term 'public order' and determining *ex post* whether the consequences of botnet attacks actually violated public order is to be done by judicial practice separately in every case.

> *§ 7^{2}. Public order*
> *(1) Public order is a state of the society in which law is being abided by and the subjective rights and legal rights of persons are being protected.*

If a violation of public order has been established and the person responsible for public order fails to remove the danger to or eliminate the violation of public order within a certain time period allocated by the police, the police may perform the obligation on behalf and at the expense of the owner in accordance with the Substitutive Enforcement and Penalty Payment Act[132].

> *§ 11. Substitutive enforcement*
> *(1) If, during the term prescribed in a warning, an addressee fails to perform an obligation imposed on the addressee by a precept and the obligation is not inseparably bound to the addressee, the competent administrative authority may perform the obligation at the expense of the addressee or organise the performance of the obligation by a third party (substitutive enforcement).*

The same act provides for substitutive enforcement which does not require a precept, warning or enforcement order. This is possible when imminent danger to public security or public order needs to be eliminated immediately. Therefore, if the danger caused by a botnet is considered imminent, the supervisory authority can take any necessary measure to eliminate the danger.

> *§ 12. Special cases of substitutive enforcement*
> *(1) Substitutive enforcement may be applied without a precept, warning or enforcement order if imminent danger to public security or order needs to be eliminated immediately.*

Similar provisions also exist under German law. The mandate of the Federal Police covers the protection of the public against threats as defined on a federal level and which concern the basic fundamental rights (§ 70 of the Federal Police Code) such as physical integrity (Art. 2(2) of the Basic Law), freedom of the person (Art. 2(2) of the Basic Law), freedom of movement (Art. 11(1) of the Basic Law) and the inviolability of the home

[132] Substitutive Enforcement and Penalty Payment Act. 9 May 2001. – RT I 2001, 50, 283; RT I, 23.02.2011, 3.

(Art. 13 of the Basic Law). Measures which infringe the confidentiality of telecommunication systems are therefore not covered by the Federal Police Code.[133]

Although fighting against botnets might more likely be a federal case due to, but not limited to, their extensive geographical reach, the primary jurisdiction falls within the competence of the regional Länder Police (e.g. Nordrhein-Westfalen (NRW)). However, even the authority given to the Länder Police is limited according to § 7 of the Länder Police Code (NRW) by the same standards as in § 70 of the Federal Police Code.

In a case where a botnet has been detected, the police may act according to the police law of the federal states to take the C&C server down, provided that there has been a danger to the public security or a threat to life or physical integrity, and upon an appropriate enforcement order (e.g. search orders (§§ 41, 42 Länder Police Code (NRW)) or an order for the confiscation of the server (§§ 43, 44 Länder Police Code (NRW)). Measures which concern the confidentiality of telecommunication systems are not appropriate for the takedown of C&C servers. Obliging an ISP to disconnect the C&C server might also fall under the right of confiscation (§ 43 Länder Police Code (NRW)) because of it being a less intensive interference, and therefore appropriate (§§ 2, 3 Länder Police Code (NRW)).

Furthermore, the takedown of the C&C server could be justified by the general provision of the Länder Police Code (§ 1 Länder Police Code (NRW)), if the botnet attacks in question constitute a danger to the public security or a violation of the public order. In such a case the police can require the botmaster, the person in charge of or hosting the C&C server, the ISP, as well as every single owner of an infected computer to terminate the activity, although the latter would be inefficient and therefore extremely unlikely.

If the person responsible for the danger to the public security or the violation of the public order refuses or fails to remove the danger or eliminate the violation of the public order within a certain time period allocated by the police, the police may perform measures of substitutive enforcement (§ 52 Länder Police Code (NRW)) at the expense of the responsible person or prescribe compulsory measures (§§ 50, 51, 53-56 Länder Police Code (NRW)). Contrary to Estonian legislation, compulsory measures and substitutive enforcement require a precept warning, if possible (§§ 56, 61 Länder Police Code (NRW)).

Another measure, although rather controversial, is the online search order, in which the police use a trojan to infiltrate a computer system to search for data or to monitor keystrokes, communication or the users' behaviour.[134] In 2007, the German Federal Supreme Court decided that a legal basis for an online search order for repressive measures does not exist in the German legal system.[135] The court set out that the online search order constitutes an intensive infringement of the basic right of informational self-

[133] *Durner*, in: *Maunz/Dürig*, Grundgesetz-Kommentar, 2012, Art. 10 GG, comment no. 197; *Mann/Müller*, ZRP 1995, pp. 180, 185.

[134] *Park*, Handbuch Durchsuchung und Beschlagnahme, 2. Aufl., 2009, comment no. 765.

[135] *BGH*, Beschl. v. 31.01.2007 – StB 18/06, NJW 2007, pp. 930; *Park* (*supra nota* 134), comment no. 766.

determination (Art. 2(1), Art. 1(1) of the Basic Law).[136] In 2008, the German Federal Constitutional Court ruled on the lawfulness of online search orders as a preventive police measure. The court characterised the online search order as a serious infringement of the basic right to the guarantee of the confidentiality and integrity of information technology systems, which the court deduced from the basic personal rights.[137] To justify such a serious infringement, a legal basis should be provided in the constitution, which to date does not exist.[138] Therefore, utilising online search orders to counter botnets is not a lawful option today.

Furthermore, the ISP in whose network the C&C server is hosted has the right to disconnect the server and even to terminate the contract with the customer in accordance with § 314 of the German Civil Code.

> *§ 314. Termination, for a compelling reason, of contracts for the performance of a continuing obligation*
> *(1) Each party may terminate a contract for the performance of a continuing obligation for a compelling reason without a notice period. There is a compelling reason if the terminating party, taking into account all the circumstances of the specific case and weighing the interests of both parties, cannot reasonably be expected to continue the contractual relationship until the agreed end or until the expiry of a notice period.*
> *(2) If the compelling reason consists in the breach of a duty under the contract, the contract may be terminated only after the expiry without result of a period specified for relief or after a warning notice without result. Section 323(2) applies with the necessary modifications.*
> *(3) The person entitled may give notice only within a reasonable period after obtaining knowledge of the reason for termination.*
> *(4) The right to demand damages is not excluded by the termination.*

The right of the ISP to take down a C&C server may also be stated in the contractual terms and conditions of the ISP. In fact, nowadays this is already the case in the majority of the terms and conditions for internet services.

Using unauthorised force to take down a C&C server

As administrative law creates opportunities for the lawful takedown of botnets' C&C infrastructure, criminal law provides for opportunities to hold accountable persons who illegally do or try to do the same thing. With regard to criminal liability, disabling the C&C server is an activity which could constitute an offence under several sections of the Estonian Penal Code. All cyber crimes in the Estonian Penal Code are based on the Council of Europe Convention on Cybercrime and the correlation is as follows:

a. Section 206 in the Penal Code deals with interference in computer data and

[136] *Park* (*supra nota* 134), comment no. 767.

[137] *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, BvR 595/07; *Park* (fn 134), comment no. 768.

[138] *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, BvR 595/07, comments no. 207, 247, 257; *Park* (*supra nota* 134), comment no. 768; *Cornelius*, in: *Leupold/Glossner* (ed.), Münchener Anwaltshandbuch IT-Recht, 2. Aufl., 2011, part 10 II. 4., comment no. 421.

conforms to Article 4 (Data Interference) of the Convention on Cybercrime.

> *§ 206. Interference in computer data*
> *(1) Illegal alteration, deletion, damaging or blocking of data or programmes within computer systems, or illegal uploading of data or programmes into computer systems is punishable by a pecuniary punishment or up to three years of imprisonment*,

A typical example of this offence is a defacement attack.

b. Section 207 in the Penal Code deals with hindering the operation of a computer system and conforms to Article 5 (System interference) of the Convention of Cybercrime.

> *§ 207. Hindering of operation of computer system*
> *(1) Illegal interference with or hindering of the operation of a computer system by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to three years of imprisonment.*

This provision was drafted with primarily DDOS attacks and spamming in mind.

c. Section 217 in the Penal Code deals with unlawful use of a computer system and corresponds to Article 2 (Illegal access) of the Convention of Cybercrime.

> *§ 217. Unlawful use of computer system*
> *(1) Unlawful access to a computer system by way of removal or circumvention of a code, password or other protective measure is punishable by a pecuniary punishment or up to 3 years' imprisonment.*

A typical example of this offence is by breaking a password, gaining access to data and copying it.

Sections 206 and 207 clearly distinguish between attacks against computer data and computer systems. However, in a case where interference in computer data (§ 206) also entails hindering the operation of a computer system (§ 207), the conduct will be qualified under the latter. It must be noted that both of these sections only protect the legal rights of owners and lawful possessors of computer systems. In this context, C&C servers are to be regarded as computer systems.

The applicability of § 217 explicitly demands the removal or circumvention of a code, password or other protective measure. Thus, if taking over a certain C&C server did not require any of the aforementioned actions, this section does not apply. In practice, however, normally all botnets have some sort of protection in place, so § 217 is nearly always a restriction to be kept in mind when taking down a C&C server. As one of the few early cyber offences, § 217 was already included in the first wording of the Penal Code. After the adoption of new offences in 2008 §§ 206 and 217 became so-to-say 'competing' norms, which means that often the same conduct could be qualified under either one of them. It is up to court practice to ascertain when to prefer one or the other.

An important notion of Estonian criminal law which comes into play with regard to botnet countermeasures (with the exception of inspecting packet and traffic records) and their (seemingly) apparent illegal nature is the 'preclusion of unlawfulness'. The Penal Code states that an act is unlawful if it comprises the necessary elements of an offence prescribed by law and the unlawfulness of the act is not precluded. In other words, in certain circumstances a person who has acted in a way which is prohibited according to the Penal Code (e.g. injured a person), has not acted unlawfully due to the presence of certain circumstances (e.g. the injured person was attacking him). Self-defence is a common basis for precluding the unlawfulness of an act (§ 28).

To determine the possibility of self-defence in the context of countering botnets, it has to be ascertained whether the person taking over a C&C server was combating a direct or immediate unlawful attack against his or another person's legal rights, whether the means used in self-defence were appropriate and proportional in light of the attack and whether or not the limits of self-defence were exceeded. Taking into consideration the fact that botnets present a remarkable threat to cyber security and in many cases a great threat to the legal rights of thousands of persons, takedown of the C&C server (and also takeover of the botnet, which is discussed next) may be the only fast and possible way to prevent or put an end to causing damage. If a direct and immediate unlawful attack is launched via a botnet, the technique can be considered as self-defence, but not exceeding the limits of self-defence has to be borne in mind.[139] The Supreme Court of Estonia has held that the limits of self-defence are exceeded in a case where the person fighting a danger (botnet) is perfectly aware of (direct intent) the fact that his technique and means exceed the threat of the particular danger (or even intends to respond with excessive measures – deliberate intent), and that the damage he is creating is excessive.[140] Thus, the principle of proportionality has to be followed strictly. In conclusion, takedown of the botnet's C&C server(s), as well as other techniques, may not be unlawful, as unlawfulness can be precluded by self-defence.

German law presents similar challenges for countering botnets. Whoever[141] disables the C&C server may violate §§ 303 a, 303b of the German Penal Code.

[139] A person is deemed to have exceeded the limits of self-defence if the person with deliberate or direct intent carries out self-defence by means which are evidently incongruous with the danger arising from the attack or if the person with deliberate or direct intent causes evidently excessive damage to the attacker. An opportunity to avoid an attack or to request assistance from another person shall not preclude the right to self-defence.

[140] The Supreme Court of Estonia, Civil Chamber ruling of 25 May 2004 no. 3-1-1-38-04. P. 8.

[141] Sections 303a and 303b of the German Penal Code do not state special requirements to the commission of the offence, therefore they apply to ISPs as well as private researchers.

> *§ 303a. Data tampering*
> *(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a(2)) shall be liable to imprisonment of not more than two years or a fine.*
> *(2) The attempt shall be punishable.*
>
> *§ 303b. Computer sabotage*
> *(1) Whosoever interferes with data processing operations which are of substantial importance to another by committing an offence under section 303a(1); or entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be liable to imprisonment of not more than three years or a fine.*
> *(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.*
> *(3) The attempt shall be punishable.*
> *(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender causes major financial loss, acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or through the offence jeopardises the population's supply of vital goods or services or the national security of the Federal Republic of Germany.*
> *(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.*

The takedown of a C&C server translates into interfering with the data processing operation of a botnet (however, the suspension of internet connectivity itself constitutes no violation of telecommunication secrecy and therefore of § 206 of the German Penal Code). The takedown of C&C infrastructure would not, however, fall under §§ 303a or b if it is justified under § 34 of the German Penal Code or §§ 227, 228 of the German Civil Code as self-defence or self-redress.[142] For the takedown of a C&C server to be justified under § 34 of the German Penal Code, the need to protect a legal right is required. This could be the case when the takedown of the C&C server occurs in order to secure the functionality and stability of the ISP's internet infrastructure, which according to § 100 of the Telecommunication Code is a protected legal interest.[143] However, the defensive action, here the takedown of the C&C infrastructure, must be suitable and necessary,[144] which is to be judged on a case-by-case basis.

> *§ 34. Necessity*
> *A person who, faced with an imminent danger to life, limb, freedom, honour,*

[142] See: *Zacyk*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 303b, comment no 20; *Fischer*, in: *Fischer* (*supra nota* 79), § 303b, comment no. 19, which refers to § 303a, comment no. 13.

[143] The enumeration in § 34 of the German Penal Code is not conclusive and also contains legal assets of the general public; see: *Fischer*, in: *Fischer* (*supra nota* 79), § 34, comment no. 3a; *Ulfried/Neumann*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), vol. 1, § 34, comment no. 22.

[144] See: *Fischer*, in: *Fischer* (*supra nota* 79), § 34, comments no. 5-19; *Ulfried/Neumann*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), vol. 1, § 34, comments no. 58-63.

> *property or another legal interest which cannot otherwise be averted, commits an act to avert the danger from himself or another, does not act unlawfully, if, upon weighing the conflicting interests, in particular the affected legal interests and the degree of the danger facing them, the protected interest substantially outweighs the one interfered with. This shall apply only if and to the extent that the act committed is an adequate means to avert the danger.*

Takeover of Botnets

The takeover of a botnet implies that it is successfully infiltrated (which often goes along with breaking encryption, reverse-engineering the botnet malware and its C&C server software) and the bots are fooled into accepting orders from a fake C&C server. As a result, the botnet can effectively and quickly be destroyed by disinfecting the hosts. On top of this, sometimes a patch could be distributed to the infected workstations, removing the security vulnerability that enabled their initial infection with the malware. However, a remote clean-up could sometimes lead to performance malfunctions or a total system crash. While the takeover of botnets is a quite effective and quick solution to achieve the takedown of botnets, there are multiple legal issues to be considered before resorting to this method.

In addition to potential privacy issues as discussed above (whether relating to violating the rights to confidentiality of communications or personal data protection), taking over the botnet by using its infrastructure could also have implications under criminal law. Estonian criminal law could place such conduct or the consequences of the conduct under §§ 206 (interference in computer data), 207 (hindering of operation of computer system), 217 (unlawful use of computer system) and/or 156 (violation of confidentiality of messages), which have already been discussed.

Similar concerns would arise under German law. Sections 202a and 202c of the German Penal Code concern data espionage and the use of so called ‘hacking tools’, [145] respectively. If a botnet is taken over with the intention to eliminate it, the acting parties do not have the intention to prepare a crime but to prevent one. However, the benevolence of the actor is not relevant, because whoever gathers information or produces or acquires (hacking) tools with the intention to gain unjustified access to somebody else’s data is punishable by §§ 202c and 202a of the German Penal Code.[146] It is not necessary to demonstrate a further intention to use the gathered data for criminal actions. Given the uncertainty in judicial practice[147] on how to handle such situations, there is a certain risk of making oneself susceptible to prosecution.[148]

[145] *Fischer*, in: *Fischer* (*supra nota* 79), § 202c, comment no. 5; *Wehner*, in: *Heidrich/Forgó/Feldmann* (Eds.) (*supra nota* 78), vol. 2, C. chapter IV B. I. 3.

[146] *Fischer*, in: *Fischer* (*supra nota* 79), § 202c, comment no. 8; *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 202c, comments no. 12-13.

[147] See: *Wehner*, in: *Heidrich/Forgó/Feldmann* (Eds.) (*supra nota* 78), vol. 2, C. Chapter IV B. I. 3.

[148] *Walter/Kargl*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 202c, comments no. 12-13.

> *§ 202a. Data espionage*
> *(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment of not more than three years or a fine.*
> *(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.*
>
> *§ 202c. Acts preparatory to data espionage and phishing*
> *(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible passwords or other security codes enabling access to data (Section 202a(2)), or software for the purpose of the commission of such an offence, shall be liable to imprisonment of not more than one year or a fine.*
> *(2) Section 149(2) and (3) shall apply mutatis mutandis.*

Additional concerns may arise from third persons' rights potentially affected by such takeover, such as the violation of confidentiality of messages (§ 206 of the German Penal Code), discussed above, or breach of contractual obligations regarding the availability of services.

Once a botnet has been taken over, two common techniques to disinfect the bots are used – remote disinfection and automated disinfection. The latter is discussed in a separate chapter due to the distinctive legal issues it presents.

Similarly to the takeover of the C&C infrastructure, remotely disinfecting hosts might also fall under §§ 206, 207, 208, 217 and/or 156 of the Estonian Penal Code. In addition, § 208 – dissemination of spyware, malware or computer viruses – could become relevant in this context. Even though the intent of the actor reflects the wish to benefit the owner of the infected machine and is good-willed, all of the mentioned provisions do not *expressis verbis* prescribe a motive, aim or any other subjective element necessary, making any intent towards the following action – hereby taking over at least parts of the botnet and implementing remote disinfection – suitable as a prerequisite for sanction.

> *§ 208. Dissemination of spyware, malware or computer viruses*
> *(1) Dissemination of spyware, malware or computer viruses is punishable by a pecuniary punishment or up to 3 years' imprisonment.*

It must be noted that within the context of § 208 the term 'malware' encompasses all harmful computer programs that are intended to damage or abuse a computer and which cannot be regarded as spyware or viruses. Pretending to be the botmaster places the person who has taken over the botnet and is disinfecting bots in a situation where his conduct may not differ much compared to when maintained by malicious actors who can control the botnet remotely and advise the bots to send spam emails, harvest information, launch attacks against targets or interfere with their regular operation, rendering the infected machines unstable or unusable. Even though the purpose of the disinfection is clearly not to cause any harm, as is the case with malicious users, still, if the C&C infrastructure is programmed and instructed to further distribute and install some sort of software on other information systems, the conduct may fall under this section. As § 208 provides for an exhaustive list of activities – dissemination of spyware, malware or viruses – the disinfection of hosts, if conducted by different means, would not fall under this provision. In other words, the applicability of § 208 depends on, first, how spyware, malware and viruses are defined, and second, whether the technological means used to disinfect the hosts falls under those definitions.

Remote disinfection of hosts would be lawful if the owner of the infected host provided his or her consent for doing do. However, in such a case different potential legal risks would have to be addressed, such as liability for potential unforeseen damage caused to the computer in case the disinfection is unsuccessful or results in unwanted negative effects.

According to German law, remote disinfection of the bots could fall under §§ 202a, 303a and 303b (in case of preparation §§ 202a, 303a(3), 303b(5), 202c) of the Penal Code. Additionally, the preparation, infiltration and disinfection of the bots fulfils the conditions for data tampering, as set forth in § 303a of the German Penal Code, even if only the infection is removed and the original state restored.[149] Whether this happens to disinfect a computer system or with the intention to commit further crimes is irrelevant to the legal assessment of the action.[150] To fulfil the subjective part of the crime, the person only has to know that he is tampering with the (malicious) data on the infected machine. The good cause of disinfecting the system is only a question of preclusion of unlawfulness.[151]

If the disinfection of an infected system causes collateral damage to a computer program or the computer's operating system, it also fulfils the requirements of computer sabotage as set forth in § 303b of the German Penal Code.[152] The subjective part of the crime requires only the acceptance (*dolus eventualis*) that the disinfection process might cause damage to the installed programs or the operating system.[153] Also the preparation of those acts is punishable.

[149] Even altering data fulfils the requirements of the offence, see: *Fischer*, in: *Fischer* (*supra nota* 79), § 303a, comment no. 12; *Zacyk*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 303a, comment no. 10; *Wehner*, in: *Heidrich/Forgó/Feldmann* (Eds.) (*supra nota* 78), vol. 2, C. chapter IV B. I. 4 a.

[150] *Fischer*, in: *Fischer* (*supra nota* 79), § 303a, comment no. 14; *Zacyk*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 303a, comment no. 13.

[151] *Zacyk*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 303a, comment no. 14, which names the defence of a computer system as a possible justification due to necessity (§ 34 German Penal Code).

[152] *Supra nota* 151, § 303b, comment no. 6.

[153] *Fischer*, in: *Fischer* (*supra nota* 79), § 303b, comment no. 18; *Zacyk*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 303a, comment no. 19.

Automated Immunisation or Disinfection

Infiltrating and taking over a botnet, as discussed above, is one way to remotely disinfect its hosts. However, analysing the behaviour of a particular malware and especially looking at its self-distribution functionality normally reveals the vulnerability used to spread the infection. While every botnet is free to use any known vulnerability at a given time, it is more common to see a limited group of vulnerabilities being used for spreading. With this knowledge one could develop a 'good malware', a so-called 'white worm', which is a piece of software that uses similar self-replication and distribution techniques as the 'bad malware', particularly targeting the vulnerability in question. But instead of having a malicious payload, it enters the host system and tries to immunise it against the vulnerability as well as to disinfect the host if an infection is detected. After its release, this 'good malware' can act completely autonomously, if so desired.

From both the Estonian and German criminal law point of view, the same offences that apply to manual disinfection are taken into consideration because, as previously stated, only the physical conduct is what determines unlawfulness, not whether the intentions of the actor were benevolent or not. Previous discussion on the listed techniques indicated that their use might involve a criminal conduct.

As Estonian law also criminalises the preparation of certain computer-related crimes (crimes prescribed in §§ 206-208, 213 and 217, which with the exception of § 213 – computer-related fraud – have all been discussed above), the stakeholders also have to bear in mind the preparation aspect. It is important to note that in case of preparation, self-defence cannot be applied.

> *§ 216^1. Preparation of computer-related crime*
> *(1) A person who, for the purposes of committing the criminal offences provided in §§ 206, 207, 208, 213 or 217 of this Code prepares, possesses, disseminates or makes available in any other manner a device, program, password, protective code or other data necessary for accessing a computer system, or uses, disseminates or makes available in any other manner the information necessary for the commission of the criminal offences specified in this section shall be punished by a pecuniary punishment or up to three years of imprisonment.*

One of the difficulties which prosecutors might stumble upon when trying to qualify operating the white worm under the computer crime provisions is that since the worm is so-to-say living its own life, demonstrating the cause-and-effect relationship and tying the chain of events back to the creator of the worm could prove to be complex.[154] This is where § 216^1 could become extremely important, because it criminalises, among other things, even the preparation of a computer program.

With regard to German criminal law, since the automated disinfection routine leaves no opportunity for obtaining knowledge about the (personal) data stored on the infected

[154] This becomes extremely relevant if the white worm, contrary to what was planned, starts to cause further damage to the infected hosts.

system (in contrast to remote disinfection), §§ 202a, 202c of the German Penal Code do not apply. Nevertheless, operating a white worm could be covered by the German Penal Code provisions of computer sabotage (§ 303b) and data tampering (§ 303a).[155] The use of white worms constitutes an interference with data processing operations as well, as the worm wipes out or least manipulates the infected data. This might damage those programs or essential functions of the operating system which the virus used to hide from authentication through anti-virus software. Since such potential collateral damage is not endorsed, the automated disinfection method is a criminal act.[156]

It is important to note that acting in a good cause does not make disinfection consensual.[157] Although an implied consent would fulfil the requirements of justification, there is still a residual risk of prosecution (§ 303c of the German Penal Code). If data tampering through the use of the white worm damages other programs or (essential) functions of the operating system, the assumption of an implied consent is rather unlikely. Although a functional botnet fulfils the requirement of an imminent danger so that the principle of necessity (§ 34 of the German Penal Code) could justify the use of the white worm, there might be cases in which it is questionable, when weighing up the conflicting interests, that the use of the white worm is reasoned, especially if third parties are affected. This is even more so if less invasive mitigation tools, such as providing instructions to the owners of the bots so that they could disinfect their computers by themselves, are available.

German law also criminalises the preparation of data tampering §§ 303a (3), 202c German Penal Code and computer sabotage §§ 303b (5), 202c German Penal Code, as does Estonian law.

Botnet Mitigation Techniques under Exceptional Circumstances

Exceptional circumstances, such as an emergency situation or state of emergency enable the use of additional measures, which typically invade the constitutional rights of people to a degree that would not be acceptable under normal circumstances.

According to the Estonian Emergency Act,[158] an emergency situation may be declared, among others, as a result of a long-term interruption of the continuous operation of specific services, e.g. data communication networks. The declaration of an emergency situation renders it possible to undertake some additional appropriate measures. Relevant measures in the context of fighting botnets can under certain circumstances include entry

[155] *Wehner*, in: *Heidrich/Forgó/Feldmann* (Eds.) (*supra nota* 78), vol. 2, C. chapter IV B. I. 5.

[156] *Fischer*, in: *Fischer* (*supra nota* 79), § 303b, comment no. 18; *Zacyk*, in: *Kindhäuser/Neumann/Paefgen* (Eds.) (*supra nota* 79), § 303a, comment no. 19.

[157] *Fischer*, in: *Fischer* (*supra nota* 79), § 202a, comment no. 12.

[158] Emergency Act. 15 June 2009. – RT I 2009, 39, 262; RT I, 29.12.2011, 1.

into property[159] and duty to grant use of things.[160] Police support is guaranteed for taking the abovementioned measures.[161]

According to the State of Emergency Act,[162] a state of emergency may be declared in response to serious threats to the constitutional order of Estonia.[163] Under a state of emergency, the following measures to mitigate or restrain the consequences of botnet attacks could be relevant:

- The Government may restrict the use of means of communication;[164]
- The chief of internal defence (usually the Minister of Interior Affairs) may apply restrictions on the right to confidentiality of messages forwarded by post, telegraph or other commonly used means for persons who are believed to endanger the constitutional order of Estonia by their activities.[165]

The German Constitution acknowledges emergency rules only in the event of a state of defence (Art. 115a(l) of the Basic Law).

> *Article 115a [Definition and declaration of a state of defence]*
> *(1) Any determination that the federal territory is under attack by armed force or imminently threatened with such an attack (state of defence) shall be made by the Bundestag with the consent of the Bundesrat. Such determination shall be made on application of the Federal Government and shall require a two-thirds majority of the votes cast, which shall include at least a majority of the Members of the Bundestag.*

The definition of an attack with 'armed forces' is explicitly vaguely formulated so that it is open to any kind of forceful act which influences the functionality of the state's institutions in a harmful way.[166] The kind of weapon used is not important as long as its effects are the same.[167] A teleological interpretation of the phrase 'armed force' must inevitably come to the conclusion that new methods of attack, such as cyber attacks, are also covered by the definition.[168] This interpretation is even more reasoned as internet technologies are taking an increasingly central role in the functioning of a state, including its critical services and infrastructure. To cut cyber attacks out of the legal discussion would mean leaving the state's defence vulnerable. Furthermore, the consequences of an attack are not limited to material or personal damages – destabilising the telecommunications infrastructure could also suffice.

According to Article 115a(1) of the Basic Law, whether a situation is classified as a state of defence or not will be decided by the Bundestag and the Bundesrat. If that is not

[159] Section 25 of the Emergency Act.
[160] Section 23 of the Emergency Act.
[161] Section 30 of the Emergency Act.
[162] State of Emergency Act. 10 January 1996. – RT I 1996, 8, 165; RT I, 29.12.2011, 1.
[163] Sections 2 and 3 of the State of Emergency Act.
[164] Section 17(1) p. 14 of the State of Emergency Act.
[165] Section 20(3) p. 6 of the State of Emergency Act.
[166] *Epping*, in: *Maunz/Dürig* (Eds.), Grundgesetz-Kommentar, Art. 115a, comment no. 42.
[167] *Ibid.*, comment no. 42.
[168] *Ibid.*, comments no. 44, 45.

possible, the decision is made by the common committee of both institutions. In a state of defence the confidentiality of telecommunications can be limited in order to employ necessary countermeasures. Article 10(2) of the Basic Law also provides for a basis to restrict telecommunications secrecy.

The freedom of expression/information (Art. 5 of the Basic Law) may only be restricted, e.g. by intercepting telecommunications, in case of danger to the public security and order. The exceptions stated in the German Code of Criminal Procedure and the 16 different police codes of the German States[169] are very conservative and a careful consideration of the facts of each case is necessary. In any case a judicial decree is required.

> *Article 5 [Freedom of expression, arts and sciences]*
> *(1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship.*
> *(2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour.*
> *(3) Arts and sciences, research and teaching shall be free. The freedom of teaching shall not release any person from allegiance to the constitution.*

The conditions for intercepting telecommunications are stated in § 100a of the German Code of Criminal Procedure.

> *§ 100a. [Conditions Regarding Interception of Telecommunications]*
> *(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if*
>
> 1. *certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence; and*
> 2. *the offence is one of particular gravity in the individual case as well; and*
> 3. *other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success.*

Duty to Act against Botnet Attacks

Even though the previous discussion might create the impression that, despite good intentions to mitigate or restrict the negative effects of botnets, national legislations make

[169] *Eisele*, in: *Sch/Sch* (*supra nota* 77), § 238, comment no. 13.

it very difficult or impossible, this coin also has another side. Most of the aforementioned botnet mitigation techniques could be illegal simply because if we as a society allowed anybody to take action that is normally under the authority of the police force, we would end up having wild justice and no control over it. Therefore, the following explains which stakeholders, such as ISPs, law enforcement agencies, academic researchers, commercial enterprises or governmental organisations, are obliged by law to perform certain duties that help to secure the cyber domain. The analysis will also deliberate on whether the stakeholders can be held liable if they do not perform their law-imposed duties which directly or indirectly oblige them to act against botnet attacks.

Internet Service Providers

With regard to ISPs, the general obligations that lie on them are those of making available the benefits of the information society – access to information, e-commerce and information services. If the service provider becomes aware of danger to the service or security of the communications network, he will assume duties to defend the service and network.

On the EU level, the duties of ISPs are primarily set forth in the E-Commerce Directive,[170] the Data Protection Directive[171] and the Electronic Communications Package,[172] which includes also the Electronic Communications Privacy Directive.[173] These instruments provide for communications providers' rights and obligations with respect to managing their services and supervising their networks.

In Estonia, according to the Electronic Communications Act[174] a duty to inform the end-user about danger to the security of the communications network and also of possible

[170] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal L 178, 17/07/2000, P. 0001 – 0016.

[171] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995, P. 0031 – 0050.

[172] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Official Journal L 105, 13/04/2006, P. 0054 - 0063; Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive). Official Journal L 108, 24/04/2002, P. 0007 - 0020; Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive). Official Journal L 108, 24/04/2002, P. 0021 – 0032; Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). Official Journal L 108, 24/04/2002, P. 0033 - 0050; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). Official Journal L 108, 24/04/2002, P. 0051 – 0077.

[173] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31/07/2002, P. 0037 – 0047.

[174] Electronic Communications Act. 8 December 2004. – RT I 2004, 87, 593; RT I, 29.12.2011, 1.

means to combat the threat lies on the service provider. An infected computer can pose danger to the communications service or its security if, for example, the bot is used to steal sensitive data from other users or to hamper the operation of their computer or network.

> *§ 101. Security requirement*
> *(2) If clear and present danger exists to the security of the communications network, the communications undertaking shall immediately inform the subscriber of such danger in a reasonable manner and, if elimination of the danger by the efforts of the undertaking is impossible, also of possible means to combat the threat and of any costs related thereto.*

Despite the fact that ISPs have no legal obligation to monitor traffic, based on the Information Society Services Act[175] ISPs, if they become aware of allegedly illegal activities performed by their clients, are required to inform the competent supervisory authorities of those activities. It can be assumed that the real-life practice of ISPs is to inform the police of incidents and activities of significant importance and that minor events are left unreported. Due to Estonia's compact size and rather small network of area-experts, the ISPs and authorities have quite direct communication channels, a fact which creates a prerequisite for effective information-sharing.

> *§ 11. No obligation to monitor*
> *(3) Service providers are required to promptly inform the competent supervisory authorities of alleged illegal activities undertaken or information provided by recipients of their services specified in §§ 8–10 of this Act, and to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements.*

Additionally, the service provider, upon the request of the prosecuting authority, investigative authority, security authority or surveillance authority, has the duty to provide existing data about the user.

> *§ 11. No obligation to monitor*
> *(4) For ascertaining the truth the service provider shall submit to the prosecuting and investigative authority pursuant to the code of criminal procedure and to the security and surveillance authority pursuant to the law and during the date set by these authorities available information about the recipient of the services to whom the service provider provides information storage service.*

The obligation to provide information to surveillance and security authorities is also provided for in the Electronic Communications Act.

> *§ 112. Obligation to provide information to surveillance agencies and security authorities*
> *(1) Where adherence to the deadlines specified below is possible due to the*

[175] Information Society Services Act. 14 April 2004. – RT I 2004, 29, 191; RT I, 06.01.2011, 1.

> *nature of an enquiry, a communications undertaking is required to provide at the earliest opportunity, but not later than within ten hours after receiving an urgent enquiry submitted by a surveillance agency or security authority, or within ten working days if the enquiry is not urgent, the surveillance agency or security authority with information concerning data provided for in § 111^{1} sections 2 and 3 of this Act.*

Furthermore, the ISP is also obliged to grant access to the surveillance or security authority to the communications network.

> *§ 113. Obligation to grant access to communications network*
> *(1) Communications undertakings shall grant surveillance agencies and security authorities access to the communications network for the conduct of surveillance activities or for the restriction of the right to confidentiality of messages, correspondingly.*

According to the Information Society Services Act, in a civil proceeding, if the court so requires, the ISP has to provide the court with information about the user, such as his personal data, and details about the individual transaction relevant to the case.

> *§ 11. No obligation to monitor*
> *(5) For ascertaining the truth the service provider shall submit to the court, upon the court's written single inquiry, on the basis and pursuant to the code of the civil procedure and during the term set by the court, available information about the recipient of the services to whom the service provider provides information storage service. For the purposes of this section, single inquiry is an inquiry about the personal data of users of electronic communications services, the fact of transmission of data by the user, and the duration, mode and format of the data concerning a particular electronic mail, a particular electronic commentary or another communication session related to the forwarding of a single message.*

The Electronic Communications Act also provides for another means to minimise the negative effects caused by botnet attacks. According to this provision, an ISP is allowed to limit the availability of its services to end-users if the activities of the end-users disturb the operation of the communications network. As botnets are often used to launch distributed denial of service attacks or spam campaigns, which create a lot of traffic and thus interrupt the smooth operation of the network, implementing this provision could significantly help to minimise the effects of the attacks.

> *§ 98. Restriction of provision of communications services*
> *(1) A communications undertaking may restrict the provision of communications services to the end-user only if:*
> *3) the end-user harmfully interferes, by using the terminal equipment, with the operation of the communications network or other users of communications services.*

Specific regulations apply to ISPs forming a part of the national critical infrastructure. An ISP connected via an interconnection point to another communication undertaker is defined as a provider of vital services.[176] Providers of vital services are obliged to: prepare a risk assessment analysis of the continuous operation of vital services; prepare a plan for ensuring the continuous operation of vital services; give immediate notice to the agency organising the vital service of events significantly disturbing the continuous operation of the vital service or of an impending risk of the occurrence of such events; upon the agency's request give the agency organising the vital service information concerning the provision of the vital service; and fulfil other responsibilities assigned to them with legal acts to ensure the continuous operation of vital services.[177] Also, providers of vital services are obliged to take appropriate measures to ensure the security of those information systems used in the provision of vital services.[178]

In Germany, ISPs are not obliged to monitor network traffic pursuant to § 7 of the Telemedia Code referred to above. A general obligation for ISPs to inform authorities and users if they become aware of a computer crime does not exist. Section 138 of the German Penal Code makes it a crime if a person, upon knowledge of a planned or committed offence, fails to bring it to the attention of the authorities. However, the penal provisions related to botnets are not included in the catalogue of § 138.[179] Nevertheless, an obligation to inform the authorities about botnet activities may arise if the botnet traffic or activities are – at least indirectly – related to the crimes listed in § 138.

> *§ 138. Omission to bring planned offences to the attention of the authorities*
> *(1) Whosoever has credible information about the planning or the commission of the following offences:*
> *1. preparation of a war of aggression (section 80);*
> *2. high treason under sections 81 to 83 (1);*
> *3. treason or an endangerment of peace under sections 94 to 96, section 97a or section 100;*
> *4. counterfeiting money or securities under section 146, section 151, section 152 or counterfeiting debit cards and blank euro cheque forms under section 152b (1) to (3);*
> *5. murder under specific aggravating circumstances (section 211), murder (section 212), genocide (section 6 of the Code of International Criminal Law), a crime against humanity (section 7 of the Code of International Criminal Law), or a war crime (section 8, section 9, section 10, section 11 or section 12 of the Code of International Criminal Law);*
> *6. an offence against personal liberty in cases under section 232 (3), (4), or (5), section 233 (3), each to the extent it involves a felony, section 234, section 234a, section 239a or section 239b;*
> *7. robbery or blackmail using force or threat to life and limb (sections 249 to 251 or section 255); or*
> *8. offences creating a danger to the public under sections 306 to 306c, section 307 (1)to (3), section 308 (1) to (4), section 309 (1) to (5), section 310, section 313, section 314, section 315 (3), section 315b (3), section 316a or section 316c at a time when the commission or result can still be averted, and fails to*

[176] Sections 34(1, 2) and 37(2) of the Emergency Act; § 87(4) of the Electronic Communication Act.
[177] Section 37(3) of the Emergency Act.
[178] Section 40(1) of the Emergency Act.
[179] *Fischer*, in: *Fischer* (*supra nota* 79), § 138, comment no. 4.

> *report it in time to the public authorities or the person threatened, shall be liable to imprisonment not exceeding five years or a fine.*
> *(2) Whosoever credibly learns*
> *1. of the commission of an offence under section 89a or*
> *2. of the planning or commission of an offence under section 129a, also in conjunction with section 129b (1), 1st and 2nd sentences,*
> *at a time when the commission can still be averted, and fails to report it promptly to the public authorities, shall incur the same penalty. Section 129b (1) 3rd to 5th sentences shall apply mutatis mutandis in the case of No. 2 above.*
> *(3) Whosoever by gross negligence fails to make a report, although he has credible information about the planning or the commission of an unlawful act, shall be liable to imprisonment of not more than one year or a fine.*

Section 109(5) of the German Telecommunication Code states an obligation for ISPs to immediately inform the Federal Network Agency (*Bundesnetzagentur*) of cases of severe security violations and disturbances if they seriously interfere with the functionality of the IT-infrastructure or telecommunication services. The assessment of the situation and therefore the question of whether or not to inform the Federal Network Agency is the responsibility of the ISP. The agency can also demand detailed information about the disturbance and the planned countermeasures. If necessary, the Federal Network Agency informs the Federal Office for Information Security (BSI), the national regulatory authorities of the other EU Member States and the European Network and Information Security Agency (ENISA). The BSI is empowered to inform the public or to order the ISPs to do so.

In some cases there might be an obligation for an ISP to inform its customers affected by a botnet, provided that the ISP knows about the existence of a concrete infection on a customer's computer and this infection presents a serious danger to the customer's equipment as well as to the execution of the contracted service provision. Based on the contractual relationship between the ISP and its customer, such an obligation might also result from § 242 of the German Civil Code. According to § 242, each contractual party has a duty to perform the contract in good faith. The obligation to protect the contractual partner (i.e. customer) from damages, if appropriate and reasonable, is covered by the scope of good faith.

> *§ 242. Performance in good faith*
> *An obligor has a duty to perform according to the requirements of good faith, taking customary practice into consideration.*

<u>Law Enforcement Agencies</u>

An investigative body, such as a law enforcement agency or the Prosecutor's Office, is, according to the Estonian Code of Criminal Procedure,[180] required to commence criminal proceedings if there is reason and grounds therefor.

[180] Code of Criminal Procedure. 12 February 2003. – RT I 2003, 27, 166; RT I, 09.07.2012, 2.

> *§ 193. Commencement of criminal proceedings*
> *(1) An investigative body or a Prosecutor's Office commences criminal proceedings by the first investigative activity or other procedural act if there is reason and grounds therefor and the circumstances provided for in subsection 199(1) of this Code do not exist.*

If the investigative body or the Prosecutor's Office is able to ascertain criminal elements in the report of a criminal offence or from other information, there are sufficient grounds to commence the proceedings. For example, if the investigative body or the Prosecutor's Office receives information about a botnet infection, which might be classified under any computer crime in the Penal Code, e.g. hindering the operation of a computer system under § 207, they are obliged to commence criminal proceedings.

> *§ 194. Reasons and grounds for criminal proceedings*
> *(1) The reason for the commencement of criminal proceedings is a report of a criminal offence or other information indicating that a criminal offence has taken place.*
> *(2) The grounds for a criminal proceeding are constituted by ascertainment of criminal elements in the reason for the criminal proceeding.*

In case the investigative body or the Prosecutor's Office does not commence criminal proceedings in a situation where the victim feels they should, the victim may file an appeal with the Prosecutor's Office.

> *§ 207. Contestation of refusal to commence or termination of criminal proceedings in Public Prosecutor's Office*
> *(1) A victim may file an appeal with a Prosecutor's Office on the bases provided for in subsection 199(1) or (2) of this Code against refusal to commence criminal proceedings.*

It may also happen that while law enforcement agencies are taking action against botnet attacks, they violate the rights of third persons. The basis and procedure for the protection and restoration of rights violated through the exercise of powers of public authority and performance of other public duties and compensation for damage caused (i.e., state liability) is set forth in the State Liability Act.[181] As law enforcement authorities exercise administrative measures when lawfully disinfecting hosts, the act applies.

According to this Act, a person may claim compensation for proprietary damage caused by a measure that in an extraordinary manner restricts the fundamental rights or freedoms of the person. Therefore, the third party must suffer significant damage, which extraordinarily affects his rights and freedoms.

[181] State Liability Act. 2 May 2001. – RT I 2001, 47, 260; RT I, 13.09.2011, 9.

> *§ 16. Damage caused by lawful administrative act or measure*
> *(1) A person may claim compensation, to a fair extent, for proprietary damage caused by a lawful administrative act or measure which in an extraordinary manner restricts the fundamental rights or freedoms of the person.*
> *(2) Unless otherwise provided by law, compensation specified in subsection (1) of this section cannot be claimed to the extent where:*
> *1) the restriction of fundamental rights or freedoms was caused by the person or the restriction was in the interests of the person;*
> *2) special treatment of persons is prescribed by law;*
> *3) the person can receive compensation from elsewhere, including from insurance;*
> *4) the issue of payment of compensation is regulated by other Acts.*

The following are some examples of damage likely to occur in a case where a lawful administrative act or measure is applied in order to fight botnets:

a. system does not boot any more (simple to fix with proper knowledge);
b. system does not work any more, resulting in total loss of stored data;
c. a (business) service stops running (financial loss);
d. a critical service stops running (possible injuries or loss of life).

Whether the occurred damage amounts to the threshold foreseen in § 16 of the State Liability Act is to be determined on a case-by-case basis.

In Germany, according to the so-called principle of mandatory prosecution stated in § 152 German Code of Criminal Procedure, law enforcement agencies are obliged to take appropriate actions, provided there are sufficient factual indications about criminal activities related to botnets.

> *§ 152[182]. [Indicting Authority; Principle of Mandatory Prosecution]*
> *(1) The public prosecution office shall have the authority to prefer public charges.*
> *(2) Except as otherwise provided by law, the public prosecution office shall be obliged to take action in relation to all prosecutable criminal offences, provided there are sufficient factual indications.*

Sections 6 and 9 of the German Penal Code state that German law is applicable in cases where the impact concerns German users.[183] Thus, German law enforcement agencies are the competent authorities for the prosecution of cases where German individuals or corporate entities are affected by botnets. However, in many cases concerning botnets law enforcement might face difficulties of international criminal cooperation resulting from multiple affected jurisdictions.

According to § 160 of the German Code of Criminal Procedure the public prosecution office starts an investigation (§ 161 German Code of Criminal Procedure) as soon as it

[182] Original translation by Brian Duffett and Monika Ebinger, Translation updated by Kathleen Müller-Rostin. See the website of the German Federal Ministry of Justice at http://www.gesetze-im-internet.de/englisch_stpo/index.html.
[183] See decision of the German Federal Supreme Court: BGH 10.12.2000 StR 184/00 - BGHSt 46, 212.

obtains knowledge of a suspected criminal offence. At the end of the investigation the prosecutor has to decide whether there are enough grounds to press public charges or not.

> *§ 160. [Investigation Proceedings]*
> *(1) As soon as the public prosecution office obtains knowledge of a suspected criminal offence either through criminal information or by other means it shall investigate the facts to decide whether public charges are to be preferred.*

As the creation and employment of a botnet comprises a violation of several criminal law provisions and the factual situation justifies a reasonable suspicion thereof, the public prosecution office is obliged to press charges. If it does not fulfil this obligation, the applicant (the aggrieved person) is entitled to compel public charges (§ 172 of the German Code of Criminal Procedure).

> *§ 172. [Proceedings to Compel Public Charges]*
> *(1) Where the applicant is also the aggrieved person, he shall be entitled to lodge a complaint against the notification made pursuant to Section 171 to the official superior of the public prosecution office within two weeks after receipt of such notification. On the filing of the complaint with the public prosecution office the time limit shall be deemed to have been observed. Time shall not start to run if no instruction was given pursuant to Section 171, second sentence.*

With regard to the financial compensation for damages inflicted by the prosecution, the German Act on Compensation for Wrongful Prosecution[184] only foresees compensation for damages which are caused immediately through law enforcement, such as wrongful conviction or remand. Furthermore, only people who were wrongfully suspected or accused are compensated, not those who were indirectly affected.[185] Their compensation occurs with recourse to the general public liability policy (§ 839 of the German Civil Code, Art. 34 of the Basic Law)[186].

Researchers

According to the Estonian Penal Code, if a person (who, among others, could also be a researcher) finds out that crimes are being carried out through the use of a botnet, that person, if the crime amounts to an offence in the first degree, is obligated to report the crime, as failure to do so is punishable. All of the computer crimes in the Estonian Penal Code are offences in the second degree and thus the obligation to report does not apply to them.[187] However, botnets could also be utilised to carry out acts of terrorism – a crime in

[184] Gesetz über die Entschädigung für Strafverfolgungsmaßnahmen (StrEG) v. 08.03.1971, BGBl. I, 157, last changes: BGBl. I, 1864 v. 08.10.2010.

[185] *Meyer-Goßner*, StPO, 52. Aufl., 2009, Anh. 5, comment no. 2.

[186] *Meyer-Goßner* (*supra nota* 185), Anh. 5, comment no. 3. See also: *Sprau*, in: *Palandt* (Ed.), BGB, 69. Aufl., 2010, § 839, comment no. 140.

[187] According to § 4(2) of the Penal Code a criminal offence in the first degree is an offence for which the maximum punishment is imprisonment for a term of more than five years, life imprisonment or compulsory dissolution. According to § 2(3) a criminal offence in the second degree is an offence for which the punishment is imprisonment for a term of up to five years or a pecuniary punishment.

the first degree – as stated in § 237 of the Estonian Penal Code, and that being the case, the reporting obligation applies.

> *Penal Code*
> *§ 307. Failure to report crime*
> *(1) Failure to report commission by another person of a criminal offence in the first degree is punishable by a pecuniary punishment or up to 3 years' imprisonment.*
>
> *§ 237. Acts of terrorism*
> *(1) Commission of a criminal offence against international security, against the person or against the environment, against foreign states or international organisations or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent or interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population, is punishable by 5 to 20 years' imprisonment or life imprisonment.*

In Germany the obligation to report crimes as stated in § 138 of the Penal Code does not apply if a person has the mere knowledge of a botnet.[188] But if a person finds out that a crime which is listed in § 138 of the German Penal Code (see above) is being carried out through the use of a botnet, the obligation to report this crime exists.

<u>Enterprises</u>

The abovementioned provision concerning failure to report a crime does not apply to legal persons, such as an enterprise (incl. critical information infrastructure providers, ISPs), as they are only liable in cases provided by law. Having said this, it is important to mention that pursuant to the Estonian Penal Code, legal persons, in addition to natural persons, can and shall be held responsible for criminal offences committed by their body, a member of the body, senior official or competent representative, insofar as it is done in the interest of the legal person.

> *Penal Code*
> *§ 14. Liability of legal persons*
> *(1) In the cases provided by law, a legal person shall be held responsible for an act which is committed by a body, a member of body, senior official or competent representative thereof in the interest of the legal person.*

In Germany there is no criminal culpability of the enterprise itself. Therefore, the enterprise cannot be held responsible if it does not report a botnet. With respect to § 14 of the German Penal Code, the statutory representative of the enterprise may only be held

[188] *Fischer*, in: *Fischer* (*supra nota* 79), § 138, comment no. 4.

responsible as an indirect perpetrator if a crime is committed by himself or an employee on his behalf.

> *§ 14. Acting for another*
> *(1) If a person acts:*
> 1. *in his capacity as an organ authorised to represent a legal entity or as a member of such an organ;*
> 2. *as a partner authorised to represent a partnership with independent legal capacity; or*
> 3. *as a statutory representative of another, any law according to which special personal attributes, relationships or circumstances (special personal characteristics) form the basis of criminal liability, shall apply to the representative, if these characteristics do not exist in his person but in the entity, partnership or person represented.*
>
> *(2) If a person, whether by the owner of a business or somebody delegated by him, has been*
> 1. *commissioned to manage the business, in whole or in part; or*
> 2. *expressly commissioned to perform autonomous duties which are incumbent on the owner of the business, and the person acts on the basis of this commission, any law, according to which special personal characteristics give rise to criminal liability shall apply to the person commissioned, if these characteristics do not exist in him but in the person of the owner of the business. Within the meaning of the 1st sentence above an enterprise shall be the equivalent of a business. If a person acts on the basis of a similar commission for an agency performing public administrative services, the first sentence shall apply mutatis mutandis.*
>
> *(3) Subsections (1) and (2) above shall apply even if the act of commission intended to create the power of representation or the agency is void.*

Section 31 of the German Civil Code considers an enterprise to be accountable for the actions of its representatives, if they cause damage to a third party in carrying out the business with which they were entrusted.

> *§ 31. Liability of an association for organs*
> *The association is liable for the damage to a third party that the board, a member of the board or another constitutionally appointed representative causes through an act committed by it or him in carrying out the business with which it or he is entrusted, where the act gives rise to a liability in damages.*

As a result, enterprises, for example ISPs, are financially accountable for the (collateral) damage brought about to third parties (e.g. owners of infected computers) caused in the course of fighting against botnets. In relation to their own customers, ISPs might also be accountable on a contractual basis (§§ 280, 241(2), 278 of the German Civil Code).

ISPs who breach the duty to inform the Federal Network Agency of cases of § 109(5) of the German Telecommunication Code (discussed above) can also be fined pursuant to §§ 149(1) No. 1 and 149(2) of the German Telecommunication Code. The Federal Data Protection Code also foresees the principles for imposing fines (§ 43 of the Federal Data Protection Code), if fighting botnets violates the requirements for personal data processing.

Governmental organisations

In Estonia, CERT-EE is responsible for handling security incidents in computer networks within the Estonian top-level domain. Its task is to educate Estonian internet users on implementing preventive measures in order to reduce possible damage caused by security incidents and to facilitate responding to security threats. CERT-EE is monitoring the traffic constantly, but is not authorised to carry out specific actions or to take certain measures to eliminate intrusions or threats. It can notify ISPs of suspicious activities and the ISPs can take further action if needed.

The Department of Critical Information Infrastructure Protection (CIIP) is a department of the Estonian Information System's Authority just like CERT-EE and it coordinates the protection of Estonia's critical information infrastructure. The main task of the department is to arrange protection of the nation's critical public and private information systems at the national level. It is also responsible for compiling risk analysis and developing CIIP security measures.

As a general principle, as long as governmental organisations are not required by law to act against botnets, they cannot be held liable for not doing so. Nevertheless, it is a recognised principle of law that the governmental organisation loses its discretionary power if it can be assumed that the consequences of botnet attacks are going to be severe and as a result the governmental organisation is obliged to act, e.g. to report the botnet.

In Germany, the so-called Citizen-CERT[189] informs and warns citizens and enterprises of viruses, worms and other security gaps. Experts analyse the security of the internet and send out warnings and safety instructions via email. The German CERT is operated from the BSI – The Federal Office for Information Security. This service by the Citizen-CERT is only an informational service and there is no obligation to report botnets. As a reaction to the latest threats to the information society and the increasing importance of information and communication technology, the BSI was allocated further tasks and powers by the Act to Strengthen the Security of Federal Information Technology (BSI Act)[190].

According to § 4 of the BSI Act, the agency as a central reporting office gathers information on vulnerabilities and attack patterns for evaluation in order to create situational awareness of the security of information technology. The BSI is obliged to

[189] See: https://www.buerger-cert.de/

[190] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes v. 19.08.2009, BGBl. I, 2821.

inform the producer or service provider in advance before it makes the information public (§ 7 of the BSI Act). It also defines IT-security standards for public institutions and administration (§ 8 of the BSI Act). According to § 4(5), the regulations of data protection are not affected by the BSI Act. Therefore the BSI is allowed to log, store and use protocol data to search for signs of attacks to prepare and initiate countermeasures (§ 5 of the BSI Act). However, the Act foresees very detailed regulations for the handling of personal data. The agency is also allowed to submit the gathered information to the prosecution office if it suspects a violation of criminal law.

All of these provisions authorise the BSI to take preventive measures in the fight against botnets or other threats to IT-security. However, its legal obligations are limited to the flawless exercise of discretion. There is no general obligation to inform or to take measures, which could be claimed by the public or other affected parties.

The scope of the BSI Act is not limited to the IT-infrastructure of the Federal Government and its agencies. The phrase 'federal communication technology' in § 2(3) of the BSI Act includes connections to third parties as well. Having said that, the agency has permission to log, store and use (personal) communication data from persons or institutions who communicate with the different agencies.[191] The definition of 'security of information technology' in § 2(2) of the BSI Act is not limited to the IT-infrastructure of the Federal Government either. The BSI and the Federal Network Agency are mandated to make a catalogue of safety requirements for operating telecommunication and data processing services (§ 109(2) of the Telecommunication Code, § 2(1) of the BSI Act). Their compliance is checked periodically by the Federal Network Agency (§ 109(3) of the Telecommunication Code, § 2(2) of the BSI Act). The Federal Network Agency, however, is only concerned if there is a serious danger to the functionality of the ISPs' infrastructure or the telecommunication system itself.

Liability of Owners of Infected Hosts

If a victim of botnet attacks has suffered significant damage, naturally he will try to find ways to compensate the harm. The most logical step would be to file a report of a computer crime to the police or to detect the botmaster and file a civil claim against him. However, the obstacle that both the police in criminal proceedings and the victim in civil proceedings are likely to stumble upon is that it is very difficult to identify the botmaster. Taking this into consideration, the following discusses whether a civil claim could be filed against the owner of the infected host, who is directly linked with the victim as damage was caused by attacks originating from his computer. This legal construct has been called downstream liability in IT-related literature, but in fact damages are compensated for according to the general principles of tort law.

[191] See: Press release from the editorial department 'beck-aktuell', Datenschutzkonferenz fordert Nachbesserung am BSI-Gesetz, becklink 276455.

From the Estonian civil law perspective, a claim could be filed against the owner of an infected system under the law of delict (i.e. tort law) provided that three main prerequisites have been met: there is causation between the act and damage, the causing of damage was unlawful and the defendant was culpable of having caused damage.

> *Law of Obligations Act*[192] *(LOA)*
> *§ 1043. Compensation for unlawfully caused damage*
> *A person (tortfeasor) who unlawfully causes damage to another person (victim) shall compensate for the damage if the tortfeasor is culpable of causing the damage or is liable for causing the damage pursuant to law.*

According to § 1045 of the LOA, the causing of damage was unlawful if it: caused the death of the victim (p. 1); caused bodily injury to or damage to the health of the victim (p. 2); deprived the liberty of the victim (p. 3); violated a personality right of the victim (p. 4); violated the right of ownership or a similar right or right of possession of the victim (p. 5); interfered with the economic or professional activities of a person (p. 6); violated a duty arising from law (p. 7); or was caused by intentional behaviour contrary to good morals (p. 8). In other words, not every damage which is suffered is unlawful and justifies compensation for damage.

Whether botnet attacks fall under one of those criteria is therefore one of the first questions to be answered before claiming for compensation. Presumably one of the most likely provisions which could apply if a botnet attack occurs is damage caused due to interference with the economic or professional activities of a person (p. 6). However, it can definitely be said that not every botnet attack will fall under the scope of § 1045, due to the quite high thresholds set forth by it.

The third precondition for implementing § 1043 of LOA is that the owner of the infected system is culpable of causing damage.

> *§ 1050. Culpability as basis for liability*
> *(1) Unless otherwise provided by law, a tortfeasor is not liable for the causing of damage if the tortfeasor proves that the tortfeasor is not culpable of causing the damage.*
> *(2) The situation, age, education, knowledge, abilities and other personal characteristics of a person shall be taken into consideration upon assessment of the culpability of the person for the purposes of this Chapter.*

The culpability of the host is determined according to § 104 of the LOA, which divides culpability into carelessness, gross negligence and intent.

[192] Law of Obligations Act. 26 September 2001. – RT I 2001, 81, 487; RT I, 08.07.2011, 6.

> *§ 104. Liability in case of culpability*
> *(1) In the cases provided by law or contract, a person shall be liable for non-performance only if the person is culpable of the non-performance.*
> *(2) The types of culpability are carelessness, gross negligence and intent.*
> *(3) Carelessness is failure to exercise necessary care.*
> *(4) Gross negligence is failure to exercise necessary care to a material extent.*
> *(5) Intent is the will to bring about an unlawful consequence upon the creation, performance or termination of an obligation.*

If carelessness is failure to exercise necessary care, then the question to be asked is whether it is the end-user's due diligence to take measures which prevent his computer from becoming infected and thus part of a botnet. The appropriate standard of care may be prescribed in law, which makes ascertaining a breach of duty of care very simple. However, more often, if at all, such principles are found in, or can be derived from, non-binding lower-level instruments such as guidelines, recommendations, instructions etc.

If the duty of care cannot be derived from a binding instrument, the general principle is to be followed, according to which it has to be evaluated whether there is a duty at the abstract level, i.e. the expected conduct of an average reasonable person. In the particular context of this report, it means that one has to assess whether an average computer user takes measures to secure his computer. According to Eurostat, 65 per cent of internet users in Estonia, which is one of the lowest figures in the European Union,[193] use any kind of IT security software or tool (anti-virus, anti-spam, firewall, etc.).[194] This data indicates that an average reasonable person has taken at least one precaution to secure his computer. However, in order to defend one's machine so that it could not be turned into a bot, a combination of defences has to be implemented. More thorough statistics on the adoption of security measures would help to assess what the actual and more precise standard of care in the society is. It can be assumed that the number of end-users who have installed a comprehensive set of security measures on their computers is significantly lower than the statistics provided above.

A case from the United States dating back to 1932 points out a different perspective when determining the appropriate standard of care. In United States v Carroll Towing[195] (the 'TJ Hooper case'), Judge Learned Hand held that "[i]ndeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. /…/ Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission." Although the case dealt with industry custom, the equivalent of which could be the ordinary care of IT security organisations, the cited quote provides a good argument for motivating the statement that an end-user

[193] The average percentage in the EU is 84. Nearly one third of internet users in the EU27 caught a computer virus. Eurostat Newsrelease, 8 February 2011. Available at: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF

[194] Nearly one third of internet users in the EU27 caught a computer virus. Eurostat Newsrelease, 8 February 2011. Available at: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF

[195] United States v Carroll Towing, 60 F.2d 737 (2d. Cir. 1932).

who has not implemented basic security tools has breached his duty of care. That is, in the information society in terms of end-users' due diligence, reasonable customs have not yet formed and therefore the *status quo* or ordinary care does not embody the reasonable standard of care.[196] Not being able to meet the level of reasonable care, despite the fact that it is not the level of care of an 'average person', could thus demonstrate the end-user's negligence according to the TJ Hooper case.

Furthermore, under Estonian law of delict, considering the subjective characteristics of the tortfeasor (see § 1050(2) cited above) is permissible when determining the culpability of the tortfeasor. This means that a 30-year old office worker who has years of computing experience could be found culpable of causing damage to a third party due to his negligence (i.e., carelessness according to § 104(3)), whereas an elderly person who is not very computer-literate could not.

Although the civil process based on § 1043 is likely to be very complicated due to many practical issues, such as the high number of potential defendants and difficulties in identifying the defendants,[197] the main virtue of the potential liability lies in its deterrent effect. It is obvious that one of the most effective means to combat botnets would be via end-users, by obliging them to take certain measures to secure their computers; however, there would be no effective control mechanism to verify whether such rules are actually being followed and therefore the success of such an approach cannot be guaranteed. Furthermore, assuming that the general public does not realise the high risks associated with unprotected computers, a rigid approach on the regulatory level requiring them to suddenly take all appropriate measures would cause a great deal of confusion and upset in the society. On the other hand, if people started to realise that unless they protect their computers they might face a court case, they might have an incentive to start educating themselves on computer security and IT-related risks, and thereby the threat of delictual liability would indirectly help to promote internet security and thus also the fight against botnets.

Estonian tort law also establishes liability for damage caused by a major source of danger (§ 1056 of the LOA). In this case, liability is not dependent on the culpability of the actor and applying § 1056 only depends on whether a computer system can be regarded as a major source of danger.

[196] See also: *Henderson, S. E., Yarbrough, M. E.* Suing the Insecure?: A Duty of Care in Cyberspace. New Mexico Law Review, 2002, Vol. 32, No. 1, pp. 11-25.

[197] However, legislation provides provisions which are favourable for the plaintiff. According to § 207 (1) p. 2 of the Code of Civil Procedure "[a]n action may be filed jointly against several defendants if several persons have obligations arising from the same grounds", which means that the plaintiff does not have to file separate claims against every bot owner, but may file a joint claim. Furthermore, according to § 236(2) of the Code of Civil Procedure "[i]f the participant in a proceeding wishing to provide evidence is unable to do so, the participant in the proceeding may request the taking of the evidence by the court. Taking of evidence is an activity of the court performed with the aim to render evidence available and enable the examination thereof in the proceeding". This is done in accordance with Chapter 26 of the Code of Civil Procedure (Pre-trial taking of evidence). – Code of Civil Procedure. 20 April 2005. – RT I 2005, 26, 197; RT I, 04.07.2012, 1.

> *§ 1056. Liability for damage caused by major source of danger*
> *(1) If damage is caused resulting from danger characteristic to a thing constituting a major source of danger or from an extremely dangerous activity, the person who manages the source of danger shall be liable for causing of damage regardless of the person's culpability. A person who manages a major source of danger shall be liable for causing the death of, bodily injury to or damage to the health of a victim, and for damaging a thing of the victim, unless otherwise provided by law.*
> *(2) A thing or an activity is deemed to be a major source of danger if, due to its nature or to the substances or means used in connection with the thing or activity, major or frequent damage may arise therefrom even if it is handled or performed with due diligence by a specialist. If liability for causing damage by means of a source of danger is prescribed by law, a thing or activity similar to such source of danger is also deemed to be a source of danger, regardless of whether the person who manages the source of danger is culpable or not.*

Estonian legislation specifically regards as major sources of danger: motor vehicles (§ 1057 – liability of possessor of motor vehicle); dangerous structures or things (§ 1058 – liability of owner of dangerous structure or thing; § 1059 – liability for structure); and animals (§ 1060 – liability of keeper of animal). Section 1056 nevertheless leaves the courts quite a wide room for interpretation as to which things and actions could also be regarded as major sources of danger. For example, according to a court judgment a descending crossing gate at a parking ground, when it hit a person on the head, was not a major source of danger,[198] whereas lighting a fire in a room or in the woods should be considered as such.

If the plaintiff is able to meet the preconditions needed to implement either § 1043 or § 1056 of the LOA, it has to be determined whether he is applying for the compensation of patrimonial or non-patrimonial damages.

A typical result of a botnet attack is the unavailability of internet services, which for a service provider such as an online vendor, whose service has gone offline, probably results in patrimonial damages. However, for example, a computer user whose quality of life and emotional balance depends on the availability of certain websites will likely endure non-patrimonial damage.

> *§ 128. Types of damage subject to compensation*
> *(1) Damage subject to compensation may be patrimonial or non-patrimonial.*
> *(2) Patrimonial damage includes, primarily, direct patrimonial damage and loss of profit.*
> *(3) Direct patrimonial damage includes, primarily, the value of the lost or destroyed property or the decrease in the value of property due to deterioration even if such decrease occurs in the future, and reasonable expenses which have been incurred or will be incurred in the future due to the damage, including reasonable expenses relating to prevention or reduction of*

[198] 12 February 2007 ruling of Tallinn Circuit Court (annulled), referred to in: The Supreme Court of Estonia, Civil Chamber ruling of 31 May 2007 no. 3-2-1-54-07. P. 6.

> *damage and receipt of compensation, including expenses relating to establishment of the damage and submission of claims relating to compensation for the damage.*
> *(4) Loss of profit is loss of the gain which a person would have been likely to receive in the circumstances, in particular as a result of the preparations made by the person, if the circumstances on which compensation for damage is based would not have occurred. Loss of profit may also include the loss of an opportunity to receive gain.*
> *(5) Non-patrimonial damage involves primarily the physical and emotional distress and suffering caused to the aggrieved person.*

Despite the fact that the wording of § 128(5) sets quite a high threshold for claiming compensation for non-patrimonial damage, the Estonian Supreme Court ruled in one of its judgments that non-patrimonial damage also embraces a setback in a person's wellbeing, which is caused by restrictions and limitations to the person's activities and way of life.[199]

Compensating patrimonial damage is made complicated by the fact that it is difficult to calculate the exact figures. This was also proven in 2007, when Estonian private sector and governmental websites were taken offline by DDOS attacks and exact damages were never calculated or announced. The compensatory amount for non-patrimonial damages is to be determined by the court based on its conscience, while taking into account all facts and circumstances.

> *Law of Obligations Act*
> *§ 127. Purpose and extent of compensation for damage*
> *(6) If damage is established but the exact extent of the damage cannot be established, including in the event of non-patrimonial damage or future damage, the amount of compensation shall be determined by the court. /.../*
>
> *Code of Civil Procedure*
> *§ 233. Evaluation of amount of claim*
> *(1) The court shall decide on the amount of damage according to the conscience of the court and taking account of all circumstances, if causing of damage has been established in a proceeding but the exact amount of the damage cannot be established or establishment thereof would involve major difficulties or unreasonably high costs including, if the damage is non-patrimonial.*

Similarly, the general precondition for claiming for damages under German civil law is that the owner of the infected system is culpable of causing damage (§ 823 of the German Civil Law).

[199] The Supreme Court of Estonia, Civil Chamber ruling of 8 February 2001 no 3-2-1-1-01. P. IV.

> *§ 823. Liability in damages*
> *(1) A person who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable to make compensation to the other party for the damage arising from this.*
> *(2) The same duty is held by a person who commits a breach of a statute that is intended to protect another person. If, according to the contents of the statute, it may also be breached without fault, then liability to compensation only exists in the case of fault.*

The culpability of the host is determined according to § 276 of the German Civil Code, which divides culpability into intent and negligence.

> *§ 276. Responsibility of the obligor*
> *(1) The obligor is responsible for intention and negligence, if a higher or lower degree of liability is neither laid down nor to be inferred from the other subject matter of the obligation, including but not limited to the giving of a guarantee or the assumption of a procurement risk. The provisions of sections 827 and 828 apply with the necessary modifications.*
> *(2) A person acts negligently if he fails to exercise reasonable care.*
> *(3) The obligor may not be released in advance from liability for intention.*

Negligence covers both carelessness and gross negligence.

Provided that carelessness might mean the failure to exercise necessary care, it is of importance whether the end-user is obliged to take measures preventing his computer from getting infected and turned into a bot.

In a case related to the misuse of an open wireless network, the German Federal Supreme Court ruled[200] that the owner of a wireless network cannot be liable for damages resulting from the illegal down- and upload of music. In the respective case the owner of the network was able to prove that he was on holiday when the alleged copyright infringements took place. The Court argued, however, that the network owner had to bear some responsibility for the actions of a third party using his system. Internet users need to secure their private wireless connections by password to prevent unauthorised usage of their internet access to commit copyright violations. Against this background, the owner of the infected computer might not be liable for damages, but he still has to take appropriate measures to prevent his computer from botnet infections, e.g. by using anti-virus software.

In any case under § 1004 of the German Civil Code the victim has the right to claim for removal of the botnet infringement and injunction related to future activities.

> *Civil Code*
> *§ 1004. Claim for removal and injunction*
> *(1) If the ownership is interfered with by means other than removal or retention of possession, the owner may require the disturber to remove the interference. If further interferences are to be feared, the owner may seek a*

[200] *BGH,* 12.5.2010, I ZR 121/08.

prohibitory injunction.
(2) The claim is excluded if the owner is obliged to tolerate the interference.

Concluding Remarks

Although they have already been present for a long time, botnets are still a rapidly growing threat to users of the internet, which is why using existing and developing new, more effective ways to restrain their further spread and utilisation is critical. Direct botnet takedowns or takeovers are potentially the most successful ways to restrain botnets. However, the implementation of anti-botnet techniques should be carefully assessed against their legal admissibility. Potential restrictions to technological countermeasures may arise from basically any field of law, including administrative, civil and criminal law.

As demonstrated by this report, traffic monitoring as well as botnet takedown and takeover techniques are surrounded by an array of legal concerns, which, if not addressed properly, may invoke the liability of the botnet fighters. Personal data protection violations as well as illegally breaking the confidentiality of communications are primary concerns which relate to packet and traffic inspection, whereas unauthorised botnet takeover or takedown may fall under many criminal law provisions.

On the other hand, the law not only establishes limitations to people’s behaviour, but also requires stakeholders to take actions against botnets in certain situations, whereas the obligations are derived from general duties to act and do not specifically concern botnets. Naturally, ISPs and law enforcement agencies are the ones who carry the highest burden in this respect. As a result, for example, if the communications network of an ISP is threatened by clear and present danger, the ISP has a duty to inform the end-user about the danger; and a law enforcement agency or the prosecuting authority is required to commence criminal proceedings if elements of a crime appear. In addition, the theoretical civil liability of end-users due to its deterrent effect would indirectly promote internet security and thus make it harder for botmasters to take over computers. This goes along with the need to educate end-users about online threats, including botnets, and the information security measures they can easily take to mitigate them.

As court practice regarding botnets in general is very limited and many botnet countermeasures addressed in this report are neither explicitly permitted nor prohibited by the law, the report was only able to draw the reader’s attention to potential points of dispute and assert that if there was to be a dispute in the future, it would be up to the courts to determine the unlawfulness of the act in question. To avoid facing a potential court case, persons or organisations looking to take up anti-botnet activities should seek for appropriate legal advice beforehand. The legislators, on the other hand, should use their mandate to shape national laws so that they support rather than hinder the fight against botnets.