Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

AS/Cult (2015) 32
18 May 2015
Or. English

COMMITTEE ON CULTURE, SCIENCE, EDUCATION AND MEDIA

Increasing co-operation against cyber terrorism and other large-scale attacks on the Internet

Rapporteur: Mr Hans FRANKEN, Netherlands, EPP/CD

Draft report[1]

A. Preliminary draft resolution

1. The Parliamentary Assembly is aware of the epochal positive impact of new information technologies on all aspects of modern societies and human life. Besides these positive effects, new vulnerabilities of our societies have emerged by the growth of the Internet and other computer networks. The Assembly is alarmed by the number and magnitude of criminal attacks perpetrated in cyberspace over the past few years, undermining public trust in technological development.

2. The Council of Europe has set important international legal standards in this field though its Conventions on Mutual Assistance in Criminal Matters (ETS N° 30, 99 and 182), on the Suppression of Terrorism (ETS N° 90 and 190), on the Prevention of Terrorism (ETS N° 196) and on Cybercrime (ETS N° 185 and 189). Nevertheless, severe obstacles still hamper the investigation and prosecution of cyber offences, particularly in the context of cross-border networks, and sanctions provided for by national legislation are not always adequate. Therefore, the Assembly believes that further work is necessary at European and international levels in order to address adequately the challenges posed by cyber terrorism and other forms of large-scale attacks on and through computer systems, which threaten the national security, public safety or economic well-being of a State.

3. Having regard to relevant EU legislation, in particular the EU Convention on Mutual Assistance in Criminal Matters, the Assembly emphasises the need to further develop and coordinate international legal and practical aspects, including the following principles:

> 3.1. Requests for mutual assistance should be executed by the requested State as soon as possible, taking as full account as possible of the deadlines indicated by the requesting State. If a request cannot fully be executed in accordance with the request, the authorities of the requested State should promptly indicate the estimated time needed for execution of the request and the conditions under which it might be possible to execute the request.
>
> 3.2. Each member State should ensure that systems of telecommunications services operated via a gateway on its territory, which for the lawful interception of the communications of a subject present in another State are not directly accessible on the territory of the latter, may be made directly accessible for the lawful interception by the latter State through the intermediary of a designated service provider present on its territory. Such procedure should be accompanied by safeguards against espionage by third States.

[1] Adopted by the committee in Paris on 2 June 2015

3.3. Member States should agree on a common level of criminalisation of large-scale cyberattacks, including aggravating circumstances of those attacks, as well as on minimum standards for penalties for such attacks.

4. Although mutual legal assistance of law-enforcement authorities has to be improved and adapted with regard to the technological development, the Assembly is conscious that other fundamental rights must not be compromised, in particular the right to protection of private life and personal data under Article 8 of the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

5. Aware that certain services and infrastructures are critical for the national security, public safety or economic well-being of a State, the Assembly recommends that member States:

5.1. draw-up Internet-independent emergency plans against cyberattacks on critical services and infrastructures, such as electricity services, gas and oil pipelines, power plants, water works, telecommunication networks, airports, railways, hospitals, fire brigades, security services and the military;

5.2. install technical security measures for the protection of critical services and infrastructures on their national territory, such as the creation of closed back-up computer systems and networks which can be used in case open Internet connections are attacked or blocked;

5.3. conclude bilateral emergency agreements with neighbouring States, in order to ensure mutual assistance in case of a cyberattack on critical services and infrastructure;

5.4. establish an adequate legal framework for public-private co-operation in the defence against large-scale cyberattacks;

5.5. recognise that States are internationally responsible for taking all reasonable measures to prevent that large-scale cyberattacks are pursued by persons under their jurisdiction or emanate from their national territory;

5.6. criminalise the production, distribution and use of malware which is intended to enable individuals to prepare or launch large-scale cyberattacks.

6. Providers of critical services or infrastructure should be obliged to immediately report any large-scale cyberattack on them to the competent law-enforcement authorities of their seat State as well as the State where such attack occurred. In addition, any natural or legal person should be made aware of how to report cyberattacks on them to their competent law-enforcement authorities.

7. Producers of hardware and software should immediately inform their customers if a systemic weakness is detected which allows for large-scale cyberattacks, such as through Botnets, electronic viruses or other malware.

8. Providers of cloud computing services should set-up security measures to protect their cloud against attacks on its security and integrity which could lead to large-scale cyberattacks, such as Botclouds.

9. Providers of public websites should ensure that their sites do not contain electronic viruses or other malware, which can lead to large-scale cyberattacks. For this purpose, their webmasters should regularly apply technical devices to prevent such malware.

10. Producers and commercial sellers of computers or software should regularly inform computer owners about their possibilities, and ultimate responsibility, for ensuring the technical safety of their computers when connecting them to the Internet or other public computer networks.

11. Member States should develop binding security standards for the protection against large-scale cyberattacks as well as the public certification of such standards, possibly at European or international level.

12. The Assembly invites the Secretary General of the Council of Europe to initiate and coordinate intergovernmental action of the Council of Europe, establish co-operation programmes with the IT industry

and Internet Service Providers, and ensure closer co-operation with the European Union and the United Nations in this field of utmost importance.

B. Preliminary draft recommendation

1. Referring to its Resolution …. (2015) on increasing co-operation against cyber terrorism and other large-scale attacks on the Internet;

2. Emphasising the importance for the Council of Europe to address the globally growing challenge to the security of computer networks posed by cyber terrorism and other forms of large-scale attacks on and through computer systems, which represent a serious threat to the national security, public safety or economic well-being of a State;

3. The Parliamentary Assembly recommends that the Committee of Ministers:

3.1. invite the Parties to the Convention on Cybercrime (ETS N° 185 and 189):

3.1.1. to draft an additional protocol defining a common level of criminalisation of large-scale cyberattacks, including aggravating circumstances of those attacks, as well as on minimum standards for penalties for such attacks;

3.1.2. to draft another additional protocol on mutual assistance regarding investigative powers, which extends in particular the scope and application of Article 32 of the Convention, in accordance with the respective Guidance Note of the Cybercrime Convention Committee (T-CY) representing the Parties to the Convention;

3.2. invite the Cloud Evidence Group established by the T-CY to study the feasibility of drafting an additional protocol to the Convention on Cybercrime regarding criminal justice access to data on cloud servers;

3.3. draft legal standards on the international responsibility of States for taking all reasonable measures to prevent that large-scale cyberattacks are pursued by persons under their jurisdiction or emanate from their national territory against computer systems in another State;

3.4. increase the assistance and monitoring action regarding the implementation of the Convention on Cybercrime in domestic law and practice as well as practical measures and cooperation against large-scale cyberattacks, in particular for the benefit of member States where the practical implementation of the Convention on Cybercrime faces difficulties;

3.5. call on Austria, Bosnia and Herzegovina, the Czech Republic, Greece, Hungary, Iceland, Ireland, Italy, Malta, Monaco, Portugal, San Marino, Sweden and the United Kingdom to sign and/or ratify without further delay the Protocol of 2003 amending the European Convention on the Suppression of Terrorism (ETS N° 90 and 190), which is necessary for the entry into force of this Protocol;

3.6. transmit to their competent national ministries and authorities Recommendation …. and Resolution …. (2015) on increasing co-operation against cyber terrorism and other large-scale attacks on the Internet.

C. Explanatory memorandum by the rapporteur, Mr Hans Franken

1. Introduction

1. This report was drafted in light of the Motion for a resolution on Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet (Doc. 13319, 01 October 2013). The challenge presented by the Motion focuses on balancing the need for increased efforts by Council of Europe member States against cyberterrorism and large-scale cyber threats with respecting fundamental rights and freedoms. In an effort to contribute to the debate, this report presents a regulatory perspective on how countries could deal with large-scale attacks. To this end, it explores the following questions:

- What are large-scale cyber-attacks and botnets, how do they relate to cyber-terrorism, and how do these affect the functioning of society?
- What is the current international regulatory landscape to address large-scale cyber-attacks?
- Which legal and non-legal approaches can be suggested to improve regulators' efforts to deal with large-scale cyber-attacks?

2. The fight against cybercrime and botnets in particular involves more than criminalisation of offences. Effective mitigation of threats includes enabling effective co-operation for exchanging and analysing infection data; stimulating Internet service providers (ISPs) to inform authorities of significant security threats; discussing the legal limits of mitigation and counter-measures and exploring non-legal measures; improving the possibilities for cross-border investigation of cyber-attacks; an effective framework for urgent co-operation requests; and supporting disinfection solutions and campaigns targeting the end-user. This report cannot comprehensively address all these issues. Rather, it provides an overview of the current developments at the international level and discusses some major legal challenges around large-scale cyber-attacks. In addition, it provides policy recommendations for improving the current legal framework on cybercrime and suggestions for non-legal measures, including the potential of capacity building programmes and public-private partnerships. It also emphasises the need for a reconsideration of the perspective from which large-scale cyber-attacks are addressed by regulators.

2. Preparatory work

3. Having been appointed rapporteur by the Committee on Culture, Science, Education and Media on 4 December 2013, I participated in the European Dialogue on Internet Governance (EuroDIG) in Berlin on 12-13 June 2014. On 16-17 April 2015, I participated in the Global Conference on Cyber Space 2015, which was organised in The Hague and launched the Global Forum on Cyber Expertise on cybersecurity, cybercrime, data protection and e-governance.[2]

4. For a discussion of the subject of this report, the Sub-Committee on Media and Information Society heard Professor Yaman Akdeniz, Istanbul Bilgi University, at its meeting in Istanbul on 12-13 May 2014. Following my contacts with Professor Dr Bert-Jaap Koops, University of Tilburg, Netherlands, he prepared a background report which was presented to the Committee in Strasbourg on 29 January 2015 and constitutes the bulk of this explanatory memorandum. On 12 March 2015, the Committee on Culture, Science, Education and Media held a hearing in the Dutch Senate in The Hague with Mr Jacob Kohnstamm, Chairperson, Dutch Data Protection Authority, Mr Olivier Burgersdijk, Head of Strategy, European Cybercrime Centre (EC3), Europol, Mr Menno van der Marel, CEO, Fox-IT, Delft, Professor Bart Jacobs, Professor of Software Security and Correctness, University of Nijmegen as well as Ms Gabriella Battaini-Dragoni, Deputy Secretary General of the Council of Europe.

5. I am very grateful to all experts, and in particular Professor Koops, for their substantial contributions, which have underlined and defined the importance and urgency of Council of Europe action aimed at increasing co-operation against cyber terrorism and other large-scale attacks on the Internet.

3. Background

6. The 2013 Norton Report,[3] observing a sample of 24 countries around the world, found the scale of

[2] https://www.gccs2015.com/

[3] http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx

consumer cybercrime to be above 1 million victims daily, estimating an overall global cost of US$113 billion annually. The numbers are modest when compared to the McAfee Net Losses Study issued in June 2014.[4] Here, the security software company evaluated the global cost of cybercrime to be US$400 billion per year, counting a total of 800 million victims just in 2013. These figures have to be taken with a large grain of salt, since the methods of calculation are unclear and reports on cybercrime are often influenced by private interests of security companies that benefit from them. Nevertheless, there is consensus that cybercrime is growing and becoming more profitable on a global scale. A growing national security concern is that cyber-terrorist attacks become more prevalent and sophisticated, and that cyber-terrorists make use of large-scale attacks to target critical services and infrastructures. To ascertain the regulatory issues related to this particular issue, it is necessary first to define cybercrime, cyberterrorism and the implications of large-scale attacks.

3.1. Cybercrime

7. The misuse of computer networks for illegal purposes gave rise to a particular criminal domain, generally referred to as cybercrime. Offences committed in cyberspace, however, can take various forms, as computers can be both target and means of criminal offences. Initial typologies on cybercrime identified three categories of offences:[5]

1. computers as instruments of an offence (computer-assisted crimes);
2. computers as targets of malicious activity (computer-integrity crimes or cybercrime stricto sensu);
3. computers as the environment for committing an offence (computer-related crimes).

8. While these three categories often overlap, the overall idea behind this classic distinction is important for illustrating that traditional offences such as fraud, money laundering, and racism, have not necessarily been redefined by information systems, but migrated to a new arena, which often changes their scope and scale if not their nature.

3.2. Cyber terrorism

9. The word terrorism is used in such an inconsistent manner and in so many different areas that one should question whether terrorism itself is a unitary concept. If on the one hand the conceptualisation of terrorism remains a challenge, on the other hand counterterrorism law has precise implications, often subjecting “terrorists” to a stricter regiment of increased penalties and lowered rights. Aside from the conceptual implications of the term ‘terrorism’, the classification of an unlawful behaviour as ‘cyber terrorism’ imposes additional challenges. This is because a cyber-terrorist offence will involve committing a cybercrime offence in the first place. The question is then how to distinguish between the two. For instance, if one considers that terrorist offences are inexorably connected to a political, religious or social cause, cyber-terrorism would be a compound of two elements: the objective element of commission of a cybercrime, plus the subjective element of the motives and intentions of the perpetrator. In the absence of the subjective element, a potential cyber-terrorist offence could only be considered a violation of cybercrime law.

10. Furthermore, the attribution issue is particularly relevant to establish the applicable set of laws. Defining authorship of cyber-attacks is a complex process, which may be hindered by perpetrators using technologies to hide their traces and identity, and require solid international cooperation. For instance, consider an attack launched from computers in State A targeting the information systems of an airport located in State B. Here the lines dividing cybercrime, cyber terrorism and cyber warfare are contingent not only on digital forensics, but also on the subjective evaluation of the intention of the attacker, as well as on determining the presence of legal responsibility of a State behind the attack. This attribution challenge was particularly visible in the case of Estonia in 2007, when a DDoS (Distributed Denial of Service) attack was launched against several public and private sector information systems. In the words of the United Nations Working Group on Counter-Terrorist Use of the Internet, although Estonia was visibly under attack, it was not clear whether this was a case of cybercrime, cyber terrorism or cyber warfare.

11. Because of the difficulty of distinguishing cyberterrorism from cybercrime in general, and of establishing for a concrete attack whether it involved a subjective element of a terrorist purpose, this report will largely focus on large-scale cyber-attacks in general, which may or may not be of a terrorist character. We are primarily concerned with the effects of large-scale attacks on critical infrastructures and essential services in society, which require serious counter-measures regardless of the subjective purposes behind them.

[4] http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

[5] Koops and Robinson, Cybercrime law: A European perspective, in E. Casey (Ed.), Digital evidence and computer crime (pp. 123-183), Waltham, MA: Academic Press (2011)

3.3. Large-scale attacks and botnets

12. While a small number of computers may cause substantial damages to a targeted system, cyber-attacks are made more profitable by involving a significant network of machines. Massive attacks are thus more aggressive and therefore more likely to cause serious harm. Today, some of the most profitable cyber-attacks are made possible by manipulation of armies of infected machines, the so-called botnets.

13. The term botnet is the shorten version of “roBOT NETwork”, meaning a collection of machines (zombies) infected by a partially autonomous piece of software that can be controlled remotely (bot) by a botmaster, who manages the Command-and-Control server (C&C).[6] Examples of unlawful use of botnets include click fraud, DDoS attacks, keylogging (intercepting keyboard strokes to capture personal or financial data), warez (unlawfully distributing copyrighted works), and spam.

14. But the traditional definition of botnet with infected machines controlled by a botmaster no longer reflects the stage of sophistication and complexity of modern botnets. A more contemporary definition of botnet is one of a network of bots or “advanced malicious software that often incorporate one or more forms of viruses, worms, Trojan horses and rootkits for propagation and hostile integration into a foreign system, providing the functionality of the compromised system to the attacker as they connect back to a central server or other infected machines”.[7] While centralised botnets continue to be used, more and more botnets distribute communication protocols via decentralised structures, increasing their resilience by avoiding a single point of failure. Current forms of sophisticated botnets are structured via peer-to-peer networks (p2p botnets) where there is no single C&C controlling the activity, but infected systems performing dual zombie and C&C functions. Other creative forms of botnets have taken the form of Botclouds, in which attacks are launched via cloud services, turning cloud computing into attack vectors. If on the one hand cloud computing has brought several useful functionalities, they have also been largely fertile for botnet activities. Botclouds do not require attackers to spend much effort in spreading the bot: they can be set up on demand, at large-scale and at low cost. Furthermore, they do not rely on owners’ activities: botclouds are permanently online and free from interruption.

15. The combination of botnet capabilities and large-scale attacks bears few technical obstacles. As noted by the United Nations Working Group on Counter-Terrorist Use of the Internet, critical information infrastructures, such as the energy sector, water supply, telecommunication networks, public administration, transport, healthcare and banking, are attractive targets for powerful and widely harmful attacks.[8] This threatening scenario calls for an efficient and proportionate framework for countering large-scale cyber-attacks.

3.4. The international regulatory landscape

16. International policy and regulation of cybercrime and terrorism has been traditionally inserted in separate instruments. Nevertheless, recent events demonstrating the connection between the two areas have increasingly called for a combined strategy on countering cyber-terrorism. In the Appendix, a brief overview is given of the most relevant legal and non-legal measures undertaken at the supra-national level with particular attention to cybercrime, cyber-terrorism and large-scale attacks.

17. From this overview, it appears that the Council of Europe and EU have the most prominent regulatory responses to cybercrime. Conventions 185 (on Cybercrime) and 196 (on the Prevention of Terrorism) shape the response to cybercrime and terrorism. However, between the launch of Conventions 185 and 196 and the present moment cybercrime has evolved significantly. New forms of crime have appeared and old forms have become more complex. In that light, the question arises whether criminal activities such as botnets and large-scale cyber-attacks are currently sufficiently covered by Convention 185. Additionally, criminal procedural law issues impose severe obstacles on the investigation and prosecution of these offences, particularly in the context of cross-border networks.

18. The EU has recently adopted Directive 2013/40/EU on attacks against information systems, replacing the earlier Framework Decision on such attacks. The Directive closely follows the substantive provisions of Convention 185, but in addition sets minimum standards for penalties, including aggravating circumstances.

[6] Kassidy et al. (2011). BOTCLOUDS: The Future of Cloud-based Botnets? Available at http://homepage.tudelft.nl/68x7e/Papers/botclouds.pdf

[7] ENISA, Botnets: detection, measurement, disinfection & defence (2011)

[8] Counter-Terrorism Implementation Task Force (CTITF), Working Group Report Countering the Use of the Internet for Terrorist Purposes, New York, May 2011, available at http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf

It does not, however, regulate investigation powers. The EU's proposal for a Directive on network and information security (NIS Directive) is another important initiative, but this has yet to be finalised and adopted.

19. Within the UN, relevant for this report is the Working Group on Countering the Use of the Internet for Terrorist Purposes within the Counter-Terrorism Implementation Task Force. In a report on the challenges, best practices and recommendations on legal and technical aspects, the Working Group found botnets a special reason for concern, and pointed to several procedural law issues that hampered the investigation of large-scale botnet attacks. In its recommendations, the Working Group emphasised the importance of ensuring protection of fundamental rights, the key role of public-private partnerships (PPPs), and the need for a multi-pronged approach.

20. INTERPOL, OECD and NATO are also making important efforts in relation to cyber-attacks, but these lie more in the field of capacity-building and practical guidelines rather than effecting new regulatory approaches.

4. Legislative approaches

4.1. Substantive law

21. To enable effective prosecution of large-scale cyber-attacks in Member States, a harmonised minimum level of criminalisation of the offences is indispensable, inter alia in light of the requirement of double criminality for mutual legal assistance. A minimum form of harmonisation may not be sufficient, however. Conventions 185 and 196 have laid the foundations of the Council of Europe regulatory framework in the fields of cybercrime and terrorism and are valuable mechanisms covering unlawful behaviour. Although Convention 185 is applicable to cybercrime committed via large-scale attacks, it makes no distinction as to the type of attack in terms of level of criminalisation. An important legislative approach in terms of substantive law is to create a more fine-grained set of criminal offences, in which more serious forms of attack incur higher penalties.

4.1.1. Scale as an aggravating circumstance of a cybercrime

22. Prosecution of a specific offence launched via single-point attacks and via botnets, on the basis of the regulatory framework of the Council of Europe, could result in the same penalties. However, when considering the potential damage caused by large-scale attacks on the targeted systems together with the harm imposed on the owners of infected devices, it is reasonable for the legislator to stipulate an elevated punishment for large-scale attacks that is proportional to the threat created by the unlawful behaviour of the botmaster(s). The size of a cyber-attack could thus be interpreted as an aggravating circumstance of the crime, for it increases the severity and culpability of the criminal act. Following this argumentation, the current framework of the CoE can be improved by increasing the sanctions pertaining to large-scale attacks. While Convention 185 refrains from establishing minimum or maximum penalties for criminal offences covered therein, a guidance note on the implementation of an additional provision on the use of botnets as an aggravating circumstance could help Member States to comply with the provision in an efficient way.

23. EU Directive 2013/40/EU on attacks against information systems could serve as an example of approximating criminal law in terms by establishing higher penalties for aggravating circumstances. With respect to the earlier Framework Decision 2005/222/JHA on attacks against information systems, the Directive established higher penalties in general, in for aggravating circumstances in particular for the offences of illegal system interference and illegal data interference. According to art. 9(3) of the Directive, illegal system or data interference should have a maximum penalty of at least three years' imprisonment if the crime was committed using a botnet[9]. Art. 9(4) of the Directive stipulates that maximum penalties for illegal system or data interference have to be at least five years' imprisonment if they were committed within a criminal organisation, if they cause serious damage, or if they are committed against computers belong to a critical infrastructure.

24. These new provisions in Directive 2013/40/EU are a good example of supra-national initiatives against large-scale attacks. Nevertheless, limiting the aggravating circumstance only to illegal system inference and illegal data interference implies that not all botnet-enabled cybercrimes face an increased penalty. For instance, in a keylogging scheme the bots listen to victims' activities looking for particular pieces of personal

[9] Or otherwise using a significant number of information systems that have been affected by misuse of devices (as meant in article 7 Directive, comparable to article 6 Convention 185).

data, such as passwords and bank account information.[10] Keylogging surveillance gains access to data but does not necessarily amount to system or data interference and is arguably out of the scope of the aggravating circumstances of art. 9(3-4) Directive 2013/40/EU. Nevertheless, through their automated nature, also the use of botnets to commit illegal access or illegal interception constitute cybercrime on a large scale, and this type of crime could also be considered a large-scale attack on information systems. Since botnets can be used for many different purposes and stages of criminal offences, it could be considered to stipulate botnet use for large-scale attacks as an aggravating circumstance, incurring a higher penalty, more generally than only in relation to illegal system or data interference.

4.1.2. Serious consequences as an aggravating circumstance of a cybercrime

25. As observed above, Directive 2013/40/EU also applies causing serious damage as an aggravating circumstance in illegal system or data interference. According to recital 5, "Member States may determine what constitutes serious damage according to their national law and practice, such as disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information." This is one regulatory approach that can be considered to deal with cyber-terrorist attacks, since these are usually particularly aimed at causing serious damage, if not in actual financial cost, then at least in terms of their broader impact on society. The Council of Europe could thus also consider, through a Guidance Note, to establish a similar aggravating circumstance for cybercrimes (art. 4-5 or possibly also art. 2-3 of Convention 185) causing serious damage.

26. The same could be considered for attacks on critical infrastructure, which the EU Directive also applies as a separate ground for higher penalties. Although this has advantages in terms of clarity and signalling the importance of critical infrastructure protection, one could also argue that this ground is already subsumed by the ground of serious damage, since attacks on critical infrastructure will typically cause serious damage (and if they do not, the attack need not necessarily be considered particularly serious to warrant enhanced penalties). Focusing on serious harm instead of the type of computer being attacked has the advantage of avoiding interpretation problems as to which computers belong to the critical infrastructure in terms of art. 9(4) Directive; after all, not all computers used 'within' a critical infrastructure are related to the critical systems at issue, and it is questionable whether an attack on a computer used for human-resource management or value-added customer services of an electricity company should count as an attack on a "critical infrastructure information system".

27. Another argument should also be taken into account in the approach to stipulating "serious damage" as an aggravating circumstance. The Internet of Things is coming closer to being a reality: a world in which not only computers and smartphones, but also a variety of things are connected to the Internet: domestic appliances such as a fridge, washing machine, television, and the thermostat, as well as cars, and devices monitoring, e.g., environmental conditions, infrastructural operations, or industrial applications. Most of these devices will not be part of the basic catalogues of critical infrastructure, but attacks on these devices can cause serious malfunctioning and therewith serious damage, not only to the device itself, but also to its environment and the people therein (think of malware infecting a smart car that allows a perpetrator to remotely take over control of the car navigation). In addition, although we are nowhere near an "Internet of people" as yet, humans are also becoming more wired, with smart devices monitoring body functions and with various human implants, ranging from pacemakers and cochlear implants to bionic limbs connected to the nervous system and brain implants. These implants make also humans vulnerable to cyber-attacks, and although these would not (necessarily) be large-scale attacks, they can definitely cause serious damage. And since remote attacks on things in people's near environment as well as on humans themselves could seem particularly frightening to many people, they might become primary instruments for cyber-terrorists once the Internet of Things and human implants become more common. Although the attacks are in principle sufficiently criminalised under Convention 185, as this gives a comprehensive conceptual list of possible types of attacks on information systems, the one-size-fits-all approach in articles 2-6 of Convention 185 may not do justice to the variety of attacks in a world where everything is connected, and where attacks really differ in character from traditional attacks on old-fashioned computers.[11] Providing for aggravating circumstances for cybercrimes causing serious damages could be one fruitful way of responding to new threats posed by cyber-attacks, be they large-scale attacks, attacks on critical infrastructures, or attacks on vulnerable cyber-connected things or people.

[10] See https://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets

[11] Gasson and Koops (2013), Attacking human implants: a new generation of cybercrime, 5 Law, Innovation and Technology (2), p. 248-277.

4.2. Procedural law

28. Although substantive law can be improved somewhat to deal with large-scale cyber-attacks, the main legislative challenges lie in the area of procedural law. Most cyberattacks can be prosecuted under one or other criminal provision in most legal systems, but it is the investigation – identifying suspects and collecting sufficient evidence – that tends to be a larger bottleneck for dealing with cybercrime. This has many reasons; we focus on three issues that we consider important to highlight in this report.

4.2.1. Implementation of procedural provisions of Convention 185

29. Convention 185 has a fairly[12] comprehensive catalogue of investigation powers that Member States should enable through their legislation. The conceptually most important powers – production order (art. 18), search and seizure (art. 19) and investigation of telecommunications (art. 20-21) – are included, alongside important, low-threshold, ancillary powers for expedited preservation of data that are vulnerable to loss (art. 16-17). Generally speaking, the Convention's parties have implemented in national law the substantive legal provisions of Convention 185 more systematically and comprehensively than the procedural provisions. For example, the power to conduct a network search regulated in art. 19(2) – an extension of a search *in situ* to search computer data remotely stored in the searching authority's territory that are lawfully accessible from the premises being searched – is explicitly regulated in the laws of, for example, Germany (art. 110(3) German Code of Criminal Procedure), the Netherlands (art. 125j Dutch Code of Criminal Procedure) and the UK (art. 20 Police and Criminal Evidence Act 1984), but no equivalent explicit provision can be found in the laws of, for example, Bulgaria, Croatia, Italy or Slovenia. Interestingly, the Philippines, which is not a party to Convention 185 but has used it as a model law, has implemented art. 19(1), 19(3) and 19(4) of the Convention almost verbatim in s. 15 of its Cybercrime Prevention Act, but has not transposed art. 19(2). We think it would be useful to have a comprehensive survey of the implementation of Section 2 (Procedural law) in parties' national laws, in order to identify whether the implementation of Convention 185 indeed shows significant gaps and deficiencies, and if so, to analyse the reasons underlying this insufficient implementation.

4.2.2. Streamlining mutual assistance

30. Chapter III of Convention 185 contains important measures to streamline mutual assistance in criminal matters, which is crucial for investigating cybercrimes that very often have an international component and involve data that are particularly vulnerable to loss if they are not expeditiously secured. Besides provisions regulating various investigation powers to use mutual assistance, the establishment of a 24/7 network (art. 35) is particularly important to enable speedy contacts between states to facilitate mutual assistance. It seems that mutual assistance procedures, despite existing efforts to streamline them and despite many good contacts among states and practitioners, is still often slow, at least for the purposes of investigating cybercrimes. Evidence collection following a request for mutual assistance can still easily take a week or several weeks, if not more, during which period the data sought may well be destroyed or moved. This cannot be easily solved, but for an effective response to large-scale cyber-attacks, it is vital that mutual assistance procedures function smoothly and expeditiously.

31. It could be considered whether stronger legal measures might help; for instance, to introduce maximum response times for responding to mutual assistance requests.[13] But the obstacles in expeditious mutual assistance procedures are presumably more organisational in nature, and policy measures to stimulate investing in resources to handle mutual assistance requests, raising awareness of the importance for the overall fighting of cybercrime of expeditiously meeting such requests, and perhaps giving clear guidelines on how national authorities can set priorities, given limited resources, in dealing with such requests, might be better suited than legislative obligations that will remain a dead letter without adequate resources or mindsets with practitioners who would have to fulfil these obligations. Given that the challenge of adequate mutual legal assistance has been recognised for a long time but that procedures, as far as we are aware, are still insufficiently speedy, further research could be undertaken to understand the particular

[12] *Fairly* comprehensive, since some potentially important powers, such as a remote search (i.e., an independent search through the Internet of computers, not connected to an existing search of a place as meant in art. 19 Convention 185), are not covered by the Convention. We cannot address in the limited scope of this report the desirability of creating additional investigation powers, which is a complex issue, not the least because of the difficult trade-off of allowing new and very intrusive forms of criminal investigation and preserving the protection of fundamental rights. The question of additional investigation should be addressed in follow-up activities in the regulatory approach to combat large-scale cyber-attacks.

[13] Directive 2013/40/EU has a limited attempt in this direction, requiring states, in art. 13(1), to "indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer". This may help the requesting authority to better plan its activities, but it does not provide anything in terms of an obligation to assist within a short time-frame.

reasons underlying the problem and to come up with innovative ways to address it.

4.2.3. Cross-border access to data

32. Given the limitations of mutual assistance, as well as the problem that it is not always clear on which territory data are stored, for instance in the context of cloud computing, there is an urgent need in practice to allow some form of remote access to data by cybercrime investigators also if the data are, potentially, stored on other countries' territory. This issue is being discussed within the Council of Europe by the 'Transborder Group', an ad-hoc sub-group of the Cybercrime Convention committee on jurisdiction and transborder access to data. It investigates possibilities for an additional Protocol or Recommendation, and has proposed a number of possible solutions that might be considered for a Protocol:

1. "Transborder access with consent but without the limitation to data stored 'in another Party' (...).
2. Transborder access without consent but with lawfully obtained credentials (...).
3. Transborder access without consent in good faith or in exigent or other circumstances (...).
4. Extending a search [from the original computer being searched to connected systems] without the limitation 'in its territory' in Article 19 [paragraph 2] (...).
5. The power of disposal as connecting legal factor."[14]

33. None of these options (except perhaps the second) provides a clear direction for addressing the issue, because of the strict limits that international law sets to accessing data on the territory of another state without that state's prior consent. Only in situations where states have agreed on certain forms of unilateral access, such as art. 32(b) Convention 185 (which allows cross-border access to data with voluntary consent of the user or provider, if these can lawfully consent to providing access to the data), is such access lawful under international law; and art. 32(b) is limited in scope and not uncontested.

34. Arguably, art. 32(b) can be interpreted as already including option 2, namely to allow cross-border searches with lawfully obtained credentials (i.e., the login name and password for remote accounts, if lawfully provided by the suspect or service provider, or found, for example, on a post-it note on the suspect's desk during a lawful search), if the searching state knows that the data are stored in a state that is party to the Convention. This interpretation of the Cybercrime Convention has yet to be agreed among the state parties to the Cybercrime before it can be considered a legitimate interpretation, but this could take the form of a Guidance Note instead of a more cumbersome ratification process for a Protocol.

35. Apart from this, it is unlikely that states will be able to agree in the shorter-term on further-reaching forms of cross-border access to data, leaving law-enforcement authorities with severely limited capacity to investigate cybercrime in an increasingly interconnected and mobile era. Before this challenge can be adequately addressed, considerable preliminary work is needed, which should include formal recognition by state representatives of the problem in international platforms and bringing together the community of cyber-investigation and the community of international law, which seldom meet and often lack basic knowledge of key tenets and developments in the other field. The Council of Europe could play an important role in this respect by hosting events involving both communities to discuss this issue, thus contributing to growing awareness of law enforcement's need for some form of cross-border access to data while remaining within the limits of international law. Once the problem is sufficiently recognised and adequately framed, states can start attempting to address the problem by drawing on existing international legal regimes for a-typical areas (such as space and satellite imaging, the high seas, piracy, and port state jurisdiction) to create an alternative account of cyberspace and the cloud in which some form of unilateral action within that space would be seen as plausibly acceptable.

5. Non-legal measures

5.1. Capacity building

36. The Council of Europe has supported several law enforcement training and capacity building activities in the field of cybercrime. From 2006 to 2011, the Global Cybercrime Project (Phase 1) reached several countries worldwide, carrying out more than 110 activities aimed at strengthening criminal justice, and improving implementation and cooperation at the level of Convention 185. Capacity building programmes offer law enforcement and other relevant stakeholders the chance to ameliorate their knowledge and upgrade their techniques, by coming into contact with other experts and bringing together officers of different jurisdictions. Large-scale cyber-attacks are not the usual type of cybercrime and require law enforcement to

[14] Cybercrime Convention Committee (T-CY) (2013), *(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data* (Strasbourg, Council of Europe).

be well-trained and equipped to deal with organised or politically motivated criminals and modern malware dissemination techniques. This also implies an increased need for cooperation, as the very characteristics of large-scale attacks will almost always result in cross-border infections. The relevance of capacity building for advancing cybercrime capabilities and resilience has been part of the cybersecurity agenda of many countries and is now part of the programme of the Cyber Security Strategy of the EU.[15]

37. Notwithstanding, we could not identify specific training programmes targeting cyber-terrorism or large-scale attacks at the Council of Europe level,[16] showing the need to foster dedicated training in this area. Due to the particular risks surrounding this potential threat and the proportion of its consequences, capacity building activities on large-scale cyber-attacks are of utmost importance. There is potential room for the Council of Europe, in light of its tradition and history of advancing the rule of law, to launch a specific programme on large-scale cyber-attacks and the use of botnets, with attention to the protection of critical infrastructure, Internet of Things and cloud computing, and include the issue in related sessions and workshops in cybercrime and counter-terrorism initiatives.

5.2. Public-Private Partnerships (PPP)

38. Public-private partnerships against cybercrime are growing as they bring together different stakeholders for the public and private sectors, pooling information and expertise about threats and enabling better strategies against cybercrime. The private sector cannot be left out in the fight against cybercrime since companies involved in the Internet infrastructure and various Internet services are in the best position to, for instance, identify the launch of a DDoS attack or recognise malicious use of their infrastructure. In addition, IT security companies with their long tradition and expertise are the most capable actors to further analyse data about infections and better understand the characteristics of threats, and they could incentivise R&D of improved security tools against vulnerabilities and exploits. All in all, an efficient framework targeting large-scale cyber-attacks requires the existence of a solid and highly knowledgeable multi-stakeholder collaborative network. While no distinctive PPPs against large-scale cyber-attacks have been identified for this report, there are various examples of PPPs against cybercrime as well as against terrorism,[17] including dedicated PPPs against botnets.[18]

39. PPPs are circles of trust and are most successful when supported by reliable organisations, accredited before its partners and the general public. Since the Council of Europe holds a strong reputation in fighting cybercrime and cyber-terrorism, it can play an important role in fostering PPPs, as well as bringing together already existing initiatives. The collaboration and exchange that can be enabled via a cooperative network of PPPs in cybercrime, counter-terrorism and botnets can provide important elements to address target large-scale cyberattacks. The richness of such a framework would build on the expertise and effort already deployed by many national teams and regional organisations in different areas of crime.

6. Tilting the perspective

40. The threat of large-scale cyber-attacks seems to loom large, because we do not know the actual threat level, for lack of reliable statistics. Part of the problem of cybercrime governance is the considerable mythology surrounding it, based as our knowledge of cybercrime (or lack thereof) often is on portrayals of hackers in movies and novels and on biased reports with blown-up figures by information security companies. It would help, first of all, to have more reliable statistics available on the actual occurrence of cybercrime, such as botnet infections. Regulators should stimulate independent research into the prevalence

[15] In this regard, see ENISA's work and training material for CERTs on Large scale incident handling, available at https://www.enisa.europa.eu/activities/cert/support/exercise.

[16] With the exception of the "New typology exercise on criminal money flows on the internet: methods, trends and multi-stakeholder counteraction" launched by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) and the Russian Federation in September 2009, in the framework of the Global Project on Cybercrime (Phase 2): Activities. Yet, the report does not directly address mechanisms to target botnets. Available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/all%20activities_en.asp.

[17] "The importance of PPPs in a counter-terrorism context is explicitly recognized by the United Nations Global Counter-Terrorism Strategy, in its Section III, paragraph 13, which encourages the identification and sharing of best practices to prevent terrorist attacks on particularly vulnerable targets." United Nations Interregional Crime and Justice Research Institute. Public-Private Partnerships (PPPs) for the Protection of Vulnerable Targets
Against Terrorist Attacks: Review Of Activities And Findings, January 2009.

[18] Such as the ENISA EP3R and the Advanced Cyber Defence Centre project funded by the EU, as well as national initiatives, e.g. Botfrei.de (Germany), AbuseHub (The Netherlands), AISI (Australia), Cyber Clean Center (Japan), and the Anti-Botnet Code of Conduct (U.S).

of cybercrime, including botnet infections and large-scale attacks, in order to better prepare for policy-making in this field.

41. At the same time, even where reliable data are available, regulators should not fall into the trap of trying to reduce the risks of large-scale attacks to near-zero level, by ever more repressive measures to find and sanction perpetrators and ever more costly security measures to prevent large-scale cyber-attacks. We live in a risk society that frames social problems in terms of the risks posed and risk-reduction strategies. In this risk society, an increasing tendency can be observed towards a culture of fear, in which we let fear of bad consequences get the better of rational, disinterested assessments of the real risks involved. As the Snowden revelations suggest, governments can get carried away in implementing anti-terrorism measures without adequately assessing whether the measures are really necessary, legitimate, effective and cost-effective. Although it is an unwelcome message in a risk-averse society, people should realise that it is impossible to live in a risk-free world and that we therefore have to learn to cope with adversities, be they natural disasters, crime, or terrorist attacks. To be sure, the potential harm of terrorist attacks is large and therefore, even if the likelihood of such attacks is low, the risk is still considerable. But that does not imply that all measures to minimise this risk are warranted. The cost of measures to prevent or reduce the effects of large-scale cyber-attacks can be enormous, both in economic terms and in terms of negative impact on human freedoms and fundamental freedoms.

42. Besides being aware of living in a risk society and the consequent pitfall of policies targeted at achieving zero risk, regulators should also take into account another perspective. Policies often address the consequences and symptoms of new phenomena, but not their underlying causes. With large-scale cyber-attacks, it is easy to assume that they are a consequence of the affordances for abusing the Internet for criminal or terrorist purposes, and hence to target policy at both increased Internet security and stronger repression of Internet-based attacks. But an important underlying cause of the risk of large-scale cyber-attacks is society's increasing dependence on ICT and the Internet. Almost all societal activities nowadays are facilitated by computers and computer networks, and because of the large benefits of doing things online rather than offline, many activities are rapidly becoming dependent on information systems and the Internet infrastructure. Thus, we are creating an extremely vulnerable society. The vulnerability does not lie in the threat of cyber-attacks per se, but rather in both the scale and the cascade effects that such attacks can have on many sectors, people, and activities.

43. In that light, we think it important to somewhat tilt the perspective of the challenge of large-scale cyber-attacks. Besides asking which measures we can take to better protect our infrastructures and to better find and prosecute those who attack the infrastructures, regulators should also ask themselves to what extent they want society to become totally dependent on the Internet as a backbone of all societal activities. The Internet is and will remain insecure, no matter how many measures will be taken. Attacks will happen, include large-scale ones, with occasionally devastating effects, no matter how many measures will be taken. This implies that an important element of any reasonable cybercrime governance strategy should be increasing the resilience of society in light of an Internet infrastructure that is inevitably vulnerable to attacks. Resilience implies not only early warning and quick response systems, but also mitigating the effects of attacks on critical infrastructures. An important part of the latter is to have adequate fall-back options, in particular to have functioning and tested fall-back infrastructures in case Internet-based infrastructures are temporarily out of order. Hospitals have power generators in case the electricity net melts down. What are the fall-back options and infrastructures that European countries have for electronic banking, smart energy grids, smart transport systems, distance learning, e-government services etc.? If the need arises when a cyber-attack temporarily blocks the use of the Internet on a large scale, can we still pay with non-electronic money, use devices that function without online connections, drive 'dumb' cars, learn from a book, get a passport? If the answer is no, then any regulatory strategy to deal with large-scale cyber-attacks is likely to fail, or else to cost so much that no e-citizen or e-consumer would be willing to pay the price.

7. Conclusion

44. A major challenge in cybercrime governance today is dealing with large-scale cyberattacks, particularly, although not exclusively, those committed using botnets – large networks of infected computers. Instruments developed in the past decades to deal with cybercrime are applicable to such attacks, but not particularly appropriate to deal with the scale and new ways in which attacks are committed, including through botnets. At the same time, instruments developed to deal with terrorist attacks are capable of dealing with large-scale attacks, but are often not specifically tuned towards cyberattacks. There is room for improvement, therefore, in taking up the challenge of large-scale cyberattacks.

45. Therefore, it can be suggested considering the following regulatory measures to address this challenge:

1. Differentiating in substantive criminal law between basic forms of cybercrime (which are already well covered by Convention 185) and aggravated forms of cybercrime, in particular attacks committed using botnets and/or attacks resulting in serious damage; for the latter, harmonisation of national law could be considered, stipulating that the minimum penalties for aggravated cybercrime should be at least a certain number of years of imprisonment.
2. A comprehensive survey of the national implementations of the procedural law provisions of Convention 185, in order to identify possible gaps and deficiencies and to analyse the reasons underlying insufficient implementation.
3. Further streamlining procedures for mutual legal assistance, by investing in resources to handle mutual assistance requests, raising awareness and giving guidelines for priority-setting to deal with these requests, and possibly by introducing maximum response times for handling mutual assistance requests. Further research should be welcomed to understand the reasons why current efforts to streamlining mutual legal assistance do not seem to have been altogether successful.
4. Putting the challenge of cross-border access to data firmly on the international agenda and involving both the cyber-investigation community and the international law community in discussions on this issue, in order to contribute to growing awareness of law enforcement's need for some form of cross-border access to data while remaining within the limits of international law. An additional Guidance Note could be considered to interpret article 32(b) Convention 185 as allowing unilateral cross-border searches with lawfully obtained credentials. In a longer-term effort, a plausible account needs to be crafted of cross-border searches in cyberspace that fit within the framework of international law.
5. Capacity building particularly focused on the specifics of large-scale cyberattacks should be fostered. The CoE could launch a specific training programme on large-scale cyberattacks and the use of botnets, with attention to the protection of critical infrastructure, Internet of Things and cloud computing.
6. Combating large-scale cyberattacks cannot be done by law enforcement authorities or public cybersecurity agencies alone. Nor is this the primary responsibility of the private sector. To stimulate the effective and legitimate Public-Private Partnerships that are needed to jointly combat large-scale cyber-attacks, the CoE could approach and bring together existing PPPs in the fields of cybercrime and terrorism, foster the creation of new PPPs as part of the Council of Europe's capacity building and outreach programmes, and issue a recommendation calling upon Member States to join regional efforts and incentivise national PPPs against large-scale cyberattacks.
7. Policy measures addressing large-scale cyberattacks should be based on reliable, independently researched statistics on the prevalence of such attacks. Policy should not attempt to minimise the risk of large-scale attacks at all costs, but rather make rational and substantiated assessments of the costs (both economic costs and impact on human rights and fundamental freedoms), while being aware that risks cannot always be calculated and that risks can in any case never be completely eliminated.
8. Measures need to focus on increasing society's resilience to deal with large-scale cyberattacks, which should include taking efforts to prevent society becoming too dependent on Internet-based infrastructures. Where governments stimulate, facilitate, or condone the replacement of offline forms of interaction with online forms of interaction, care should be taken that adequate fall-back options remain available. The Internet is and will remain insecure, and cyber-attacks, small and large, will happen, no matter how many measures are taken. Society needs to be prepared to live with the consequences of large-scale cyberattacks.

Appendix: The International regulatory landscape

Council of Europe (CoE)

1. The CoE Convention on Cybercrime (ETS 185), widely known as the Cybercrime Convention (hereinafter Convention 185), presented four categories of cybercrime offences, namely: 1. Offences against the confidentiality, integrity and availability of computer data and systems; 2. Computer-related offences; 3. Content-related offences, namely child pornography (supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189); and 4. Offences related to infringements of copyright and related rights. As clarified by the Explanatory report to Convention 185, the substantive law provisions are aimed at harmonising domestic laws by establishing minimum common standards on cybercrime. Member States and other parties to the Convention were given discretion to build upon these minimum standards and expand the range in national cybercrime law. In fact, Convention 185 has been used as a model law, with several signatories opting for a broader and more comprehensive domestic approach to cybercrime, as can be seen, for instance, in the criminal codes of Switzerland, the USA and Germany.

2. Furthermore, the CoE Convention on the Prevention of Terrorism (ETS 196) (hereinafter Convention 196) adopted a broad regulatory scope without providing a specific definition of the term terrorism. As a consequence, this definition must be found in the instruments listed in the Annex of the treaty. Nevertheless, even the instruments listed in the Annex fail to provide a comprehensive and internationally accepted definition of terrorism, which has been mostly left at State discretion at domestic level.

3. The CoE has identified cyber-terrorism and use of the Internet for terrorist purposes as priority focus areas. In fact, they have been included in the agenda of the Committee of Experts on Terrorism (CODEXTER) since 2006. The CoE expert report on “Cyberterrorism – the use of the Internet for terrorist purposes” highlighted three potential uses of information systems by terrorists, in line with the typology used in Convention 185: (a) online attacks targeting critical infrastructures and human life; (b) dissemination of terrorist-related content (presentation of terrorist views, propaganda and threats, recruitment and training, fundraising and financing); and (c) other logistical uses of information systems by terrorists (online communication and target analysis). As noticed, a terrorist cyber-offence may be difficult to recognise as such, since this conduct will almost inevitably also constitute a cybercrime offence under Convention 185, with the implications discussed above.

4. The achievements of the CoE and the Convention 185 and 196 in shaping the response to cybercrime and terrorism are undeniable. However, between the launch of Conventions 185 and 196 and the present moment cybercrime has evolved significantly. New forms of crime have appeared and old forms have become more elaborate. In that light, the question arises whether criminal activities such as botnets and large-scale cyber-attacks are currently sufficiently covered by Convention 185. Additionally, criminal procedural law issues impose severe obstacles on the investigation and prosecution of these offences, particularly in the context of cross-border networks. Also, no specific provision on the protection of critical infrastructures can be found in the CoE regulatory framework on terrorism or cybercrime.

European Union (EU)

5. The 2004 EU Communication on Critical Infrastructure Protection (CIP) in the fight against terrorism demonstrated regional concerns on the potential terrorist use of information systems against critical infrastructures. The Communication refers to how cyber and physical attacks can be combined to bring critical infrastructures to fail, with substantial damage to society. As highlighted by the Communication, EU Member States’ critical infrastructures are increasingly dependent on information systems and on each other. This technological dependency has made critical infrastructure more vulnerable to interference, disruption and destruction, and infrastructure interdependency has raised concerns of cascade failure effects. The EU Counter-Terrorism Strategy has listed the development of a common approach to detect and tackle problem behaviour, in particular the misuse of the Internet, as key priority in the prevention of terrorism. The Communication on CIP in the fight against terrorism resulted in the European Programme for Critical Infrastructure Protection (EPCIP) in 2006, ultimately leading to the adoption of Directive 2008/114/EC, which set countering terrorist threats a priority.

6. More recently the Cyber Security Strategy of the European Union published in 2013 highlighted the need to improve tools and instruments to fight cyber-terrorist activities. Following the efforts to strengthen cybersecurity in the EU, a proposal for a Directive concerning measures to ensure a high common level of

network and information security across the Union (hereinafter NIS Directive) was launched, and shortly after the Directive 2013/40/EU on attacks against information systems was adopted. Moreover, the cybersecurity regulatory framework of the EU has given mandate to Europol and particularly its European Cybercrime Centre (EC3) as well as to the European Union Agency for Network and Information Security (ENISA) to act on improving prevention, resilience and response to cybercrime. In December 2013, Europol and the FBI of the USA partnered with industry and national law enforcement agencies in a consortium that led to the disruption of the ZeroAccess botnet, estimated to have infected 2 million machines around the world.

7. The original text of the proposed NIS Directive promotes an enhanced framework in case incidents against information systems are linked to cyber-espionage or state-sponsored attack, or if they have national security implications. In this scenario, early warning mechanisms will allow national security and defence authorities to timely inform relevant stakeholders about the threat so as to enable risk and crisis management and appropriate responses. Furthermore, the Directive 2013/40/EU on attacks against information systems (the so-called Botnet Directive) introduced the concept of large-scale attacks, criminalising the unlawful use of bots and increasing sanctions for specific offences committed through botnets. Directive 2013/40/EU used double criteria to classify large-scale attacks based on size and impact on the targeted system. Under Directive 2013/40/EU thus a large-scale attack is either an attack conveyed by several devices or one that causes substantial economic damage. In both cases, a specific minimum number of devices or minimum amount of economic loss has not been established, leaving the legal text open for interpretation in concrete cases. In short, Directive 2013/40/EU is an innovative instrument in the fight against large-scale attacks for enabling adequate sanctioning against powerful large-scale cyber-attacks.

8. In addition, the EU Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between Member States of the European Union provides for a legal basis for law-enforcement co-operation across borders within the European Union.

International Criminal Police Organisation (INTERPOL)

9. The International Criminal Police Organisation (INTERPOL) is the world's largest police organisation, with 190 members around the globe, actively working against cybercrime and terrorism. INTERPOL and the UN have a long history of cooperation in law enforcement and many international instruments enacted by the latter encourage Member States to seek collaboration with INTERPOL to ensure the rule of law. INTERPOL's role in combating cybercrime focuses on harmonization, capacity building and operational and forensic support. Here the INTERPOL High-Tech Crime Unit acts through global and regional cybercrime expert group meetings and training workshops, cooperating with law enforcement, industry and academia, and assisting members in cases of attacks and requests for cooperation. In the area of terrorism, INTERPOL collects, stores, analyses and exchanges data about potential terrorist activities with member countries and other international organisations.

10. While INTERPOL is not a forum for creating binding international legislation on crime, in 2005 the organisation enacted resolution AG-2005-RES-10, urging Member States to, *inter alia*, introduce national contact points within law enforcement agencies to facilitate the rapid exchange of information, to take part in international investigations, and to increase the exchange of information about international terrorist networks and their enabling methodologies, including information on the use of the Internet to support criminal activity.

North Atlantic Treaty Organisation (NATO)

11. The North Atlantic Treaty Organisation (NATO) is an international military organisation that has been actively involved in countering terrorism and in the areas of cyber defence and cyber warfare. NATO's Strategic Concepts target cyber terrorism and the protection of critical infrastructure and demonstrate the organisation's efforts in furthering prevention, detection, and defence against cyberattacks and international terrorism. To this end, NATO has offered workshops and capacity training on cyber-terrorism for Member States. More recently in 2013, NATO CCDCOE published the Tallinn Manual on the International Law Applicable to Cyber Warfare. The Tallinn Manual revisits the existing international humanitarian law to define its particular application to conflicts in cyberspace; it is today the most solid guide in cyber warfare and a good example of how organisations can improve the rule of law without necessarily engaging into creating new legislation.

Organisation for Economic Co-operation and Development (OECD)

12. The Organisation for Economic Co-operation and Development (OECD) is not particularly involved in countering crime and terrorism, but mostly involved in the area of economic growth, social development and environmental challenges. Nevertheless, the OECD acts as an observer in the Cybercrime Convention Committee (T-CY) of the CoE and has joined efforts in the field of cybersecurity. The OECD has launched Guidelines for the Security of Information Systems and Networks. More recently in 2012, the OECD published "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy". In this document, the organisation features the use of the Internet for terrorist purposes, as an example of how sources, motivations, nature, organisation and sophistication of threats are quickly evolving.

United Nations (UN)

13. Key resolutions enacted by the United Nations Security Council have brought states' attention to cyber-terrorist threats (res. 1373/2001 and res.1566/2004). In particular, res. 1624/2005 condemned use of the Internet for terrorism justification and glorification, calling upon States to prohibit by law and prevent incitement to commit a terrorist act or acts (UNODC, 2012). Other UN instruments stressing the need for improved measures against cyber-terrorism include the Security Council res. 1963/2010 and the Secretary General 2006 report to the General Assembly entitled "Uniting against terrorism: recommendations for a global counter-terrorism strategy". The SG report specifically emphasises the need to ensure promotion of the rule of law, respect for human rights, and effective criminal justice systems.

14. The UN has also joined efforts in forming a cooperative network between its agencies and other important international organisations and international actors. The Counter-Terrorism Implementation Task Force (CTITF) coordination framework harmonises United Nations (UN) efforts on the fight against terrorism, supporting the implementation of the UN Global Counter-Terrorism Strategy, adopted by the UN General Assembly in September 2006 (A/RES/60/288). Acknowledging the threat posed by terrorist use of the Internet, in Section II, paragraph 12 of the strategy, States pledged: "To work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to: (a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard." As described, the strategy acknowledged the dual role of the Internet as both means for spreading terrorist manifestations as well as for countering its dissemination.

15. The CTITF created eight working groups, focused on the main counter-terrorism areas, which included setting up a Working Group on Countering the Use of the Internet for Terrorist Purposes. The mandate of this particular Working Group includes identifying and bringing together stakeholders and partners on the issue of abuse of the Internet for terrorist purposes, such as through radicalization, recruitment, training, operational planning, fundraising and other means. In 2011, the Working Group published an overview of the challenges, best practices and recommendations on legal and technical aspects. In this particular report, the Working Group found botnets a special reason for concern. In the opinion of the Working Group, botnets can be used to commit powerful attacks, such as the one launched against Estonia in 2007. The Working Group evaluated that several procedural law issues hampered the investigation of the Estonian case. This was due to lack of effective instruments that could enable quick collection of evidence and to the limitation of procedural instruments to specific communications. This hampered the analysis of the botnet communications, as they are not necessarily established between the infected device and the command-and-control centre. The final recommendations and conclusions of the report were:

- Importance of ensuring protection of fundamental rights – States' responsibility to respect and protect human rights, and in this particular context the right to privacy, may not be overridden by the need for public safety and national security. Rather a balance between the counter-measures and techniques against cyber-terrorism and the right to privacy must be ensured;
- Key role of public-private partnerships (PPPs) – as telecommunications infrastructures and information systems are manufactured, owned, or distributed by private sector, and given private-sector expertise in fighting cyber threats, creating networks of cooperation between public authorities and business is of utmost relevance. PPPs have the potential to bring together expertise from different sectors and share critical information about cybercrime to improve prevention, resilience and disinfection of information systems; and

- Multi-pronged approach – as legal and technical measures have limited effectiveness in themselves, a holistic approach to tackling cyber-terrorism in all its sources must include awareness programmes to educate citizens and discredit terrorist organisations.

16. As described, counter-terrorism efforts led by the United Nations are managed at the level of the CTITF. Nevertheless, other UN agencies have played an important role in strengthening policy on cyber-terrorism-related issues. The United Nations Offices on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) participate in the CTITF and are active contributors to policy and high-level discussions on issues related to cybersecurity and cybercrime.