EuroDIG
European Dialogue on Internet Governance

European Dialogue on Internet Governance 2008 – 2020

Security and Crime: A Decade of Change

Sharing responsibilities and getting the balance right through inclusive dialogue

Tatiana Tropina

European Dialogue on Internet Governance 2008 – 2020

Security and Crime: A Decade of Change

Sharing responsibilities and getting the balance right through inclusive dialogue

Tatiana Tropina

About EuroDIG

Launched in 2008, EuroDIG, the European Dialogue on Internet Governance, is a unique annual event that brings together Internet stakeholders from throughout Europe (and beyond), and from across the spectrum of government, industry, civil society, academia and the technical community. Stakeholders and participants work over the course of each year to develop, in a bottom-up fashion, a dynamic agenda that explores the pressing issues surrounding how we develop, use, regulate and govern the Internet. EuroDIG participants come away with broader, more informed perspectives on these issues and new partners in responding to the challenges of the information society.

Content

Foreword

Marina Kaljurand – Member of the European Parliament and former Estonian Minister of Foreign Affairs

EuroDIG (European Dialogue on Internet Governance) was launched in 2008 and since then has established itself as an open and inclusive arena for internet governance discussions, including cybersecurity.

EuroDIG is known for its multistakeholderism and attracts a growing number of different stakeholders every year. EuroDig is recognized as an independent and respected forum. It represents the new reality of inclusiveness in terms of fostering multi-stakeholder dialogue about cybersecurity (as well as other digital topics). This public-private-partnership is not a slogan but an example of real cooperation between governments, industry, academia, civil society and the tech community. To this list, I would also add parliaments and parliamentarians. They are the voice of the people; and they are both accountable to and legislative on behalf of citizens. Therefore, I find that the parliamentary track launched at IGF 2020 is particularly important and timely. We need digitally educated politicians to adopt digitally competent laws.

I see it in my daily work in the European Parliament. The European Union has launched an overly ambitious digital agenda – A Europe Fit for Digital Age. It will have an impact on all

our lives and almost all spheres of life. It entails the adoption of a wide range of new legislation and the European Parliament's role cannot be underestimated in this process. The European Parliament advocates for a robust and advanced digital policy and has continuously helped to maintain the focus on digital issues, including cybersecurity. I would argue that today every Parliamentary Committee has either a direct or an indirect connection to digital topics. As such, I hope that EuroDIG will also have its own parliamentary track to promote discussion on all aspects of digital governance.

I first attended EuroDIG in 2015 in Sofia and liked what I saw. As an Undersecretary and Ambassador, I had attended hundreds of international conferences, usually following the same pattern – rushing in, delivering remarks and rushing out. Always busy, always on the run, and almost always meeting the same conference crowd. My EuroDIG experience was different. I took my time, listened and talked, not only during official presentations, but also during coffee breaks and social events. I enjoyed it, and I learned a lot about the importance of listening to every stakeholder.

I am proud that my country – Estonia – hosted EuroDIG in 2017. The theme was DIGital futures: promises and pitfalls. It was a unique opportunity for my country to demonstrate our proud achievements in terms of e-Estonia and e-lifestyle.

I still have my notes from the panel I shared with Kaja Ciglic (Director, Government Cybersecurity Policy and Strategy, Microsoft), George Jokhadze (Cybercrime Programme Office of the Council of Europe) and Sally Wentworth (Vice President of Global Politics Development, ISOC).

The introduction to our panel was as follows: *Cybersecurity threats make it to the daily headlines: massive DDoS attacks against DNS Service, alleged elections hacks, espionage, terrorism and cyberwarfare. How does this change the cybersecurity landscape and influence the perceptions and actions of different stakeholders?*

EuroDIG was established one year after Estonia became the first country in the world to be subject to a politically motivated cyberattack against a sovereign nation, so cybersecurity has been on the EuroDIG agenda from the very beginning. Those D-DOS in 2007 were primitive by today's standards. They did not destroy anything or hurt anybody, but they were humiliating and disturbing for a country that was known for its e-lifestyle. However, our resilience was proof-tested and we learned valuable lessons, which we have been sharing ever since.

What were the main lessons learned?

Firstly, the importance of political decision-making and having cybersecurity high on the political agenda.

Secondly, the importance of having our house in order – which entails a strong legal framework, strategies/action plans with a clear division of responsibilities imbedded into the working plans of ministries/agencies with annual reporting obligations.

Thirdly, the importance of international co-operation. Cyberattacks do not have borders and so neither should cybersecurity. On the contrary, international cooperation at all levels and in different formats is crucial in order to face and to tackle existing and emerging cybersecurity challenges.

Finally, last but not least, the importance of an inclusive approach. For the first time in the history of mankind, Governments cannot be effective in the cybersecurity sphere without the support of and cooperation with other stakeholders: whether they are industry/private sector, academia, civil society, or the tech sector. Collaboration between the private and public sectors has always been at the centre of Estonian innovation. In the 90s, the government started several IT programs as a catalyst, but only in a few cases was it the main sponsor. Since the early nineties, the government's philosophy was not to hire programmers, but to use the services of private companies, which in turn increased the competitiveness of the Estonian IT sector. We called it an all-nation approach. Today we call it public-private partnerships, inclusiveness, multistakeholder models etc.

I am glad that a multistakeholder approach has finally been established and recognized as a new reality of digital cooperation, also in the field of cybersecurity. At least we can observe it based on political statements. The Paris Call for Trust and Security in Cyberspace launched by President Macron in 2018 "calls for all cyberspace actors to come together to face digital threats endangering citizens and infrastructure" and "encourages states to cooperate with private sector partners and civil society." The Report of the UN Secretary-General's High-level Panel on Digital Cooperation "considered models of digital cooperation to advance the debate surrounding governance in the digital sphere." The report states in the Executive Summary that "effective digital cooperation requires that multilateralism, despite current strains, be strengthened. It also requires that multilateralism be complemented by multi-stakeholderism – cooperation that involves not only governments but a far more diverse spectrum of other stakeholders such as civil society, academics, technologists and pri-

vate sector." This understanding is one of the cornerstones of the Report and was reiterated in the UN Secretary-General's Roadmap for Digital Cooperation.

It is fair to say that EuroDIG has contributed significantly to the wider acceptance of multistakeholderism – not only by statements but also by example. The future of digital cooperation and the multistakeholder model (MSM) have been on digital agenda for years. Finally, it seems that national and international actors have accepted it and see its benefits. However, there are still open questions, starting with who should be included in the MSM and how exactly MSM should take place. We have to continue these discussions, also at EuroDIG.

European Dialogue on Internet Governance 2008 – 2020. Security and Crime: A Decade of Change. Sharing responsibilities and getting the balance right through inclusive dialogue by Dr Tatiana Tropina is unique and symbolic.

Unique, because it captures the first 12 years of EuroDIG, from 2008 – 2020. As Tatyana writes: "The report has taken a chronological approach to show the developments in the cybersecurity discussions and to illustrate how EuroDIG has most of the time followed – year after year – the issues that were the most relevant for Europe's cybersecurity agenda.".

Symbolic, because it ends with 2020 – a year when the world confronted the COVID-19 pandemic which changed the world and how we look at digital topics, including cybersecurity.

This book is an excellent read for a wide audience interested in EuroDIG discussions about cybersecurity. It is comprehensive and educational and it presents the views of a wide range of different stakeholders, in just the same way that EuroDIG operates.

In 2020, EuroDIG was held for the first (and hopefully last) time fully online. We, EuroDIG fans and supporters, were supposed to meet in Trieste but we met only virtually. Online meetings have become the new normal, but they have not replaced face-to-face meetings, quick chats during coffee breaks, or social gatherings. I hope that EuroDIG will return soon to its traditional way of working.

I would like to wish EuroDIG interesting discussions on timely topics with a growing number of participants for many years to come.

Thank you, Tatiana! This is your first book about EuroDIG and cybersecurity. Hopefully, there will be a sequel to follow.

Marina Kaljurand
April 2021

Introduction

Dr. Tatiana Tropina, Subject Matter Expert for security and crime at EuroDIG[1]

Cybersecurity issues have been high on the agenda of all Internet stakeholders since the term "Internet governance" was first coined nearly 20 years ago when the approach to governing the global network was broadened from the technical management of Internet identifiers to include a much broader range of public policy issues.

The emergence of cybersecurity as one of the key considerations for policymakers can be traced back to the first report of the Working Group on Internet Governance (WGIG) which was a United Nations multistakeholder working group created after the first phase of the UN World Summit on the Information Society (WSIS) in 2003. Their report in 2005 identified "Internet stability, security and cybercrime" as one of the most relevant public policy concerns.

The increased dependency since the WSIS of many aspects of human life on information and communication technologies has not only increased the relevance of cybersecurity to Internet governance but also brought various

stakeholder communities – for example national security agencies, telecommunications administrations and financial regulators – into international debates on Internet governance.

The European regional multistakeholder Internet governance forum, the European Dialogue on Internet Governance – EuroDIG – has facilitated multi-stakeholder discussions about many varied aspects of cybersecurity since its first open meeting in Strasbourg in 2008. In the following years the cybersecurity discussions at EuroDIG have developed and matured in the course of EuroDIG's development as the unique regional forum for all stakeholders to address the opportunities and challenges associated with the Internet's evolution as the global platform for the digital revolution. This report aims to provide a comprehensive overview of how cybersecurity discussions at EuroDIG have evolved since its inception up to the present time when the global COVID-19 pandemic has revealed how vulnerable people and businesses are to security threats online and how important it is to have trust in a safe and secure Internet.

The report's chronological review illustrates how EuroDIG has generally succeeded in keeping in step with market and technology developments as a multistakeholder forum for discussing the issues that have emerged as most relevant for Europe's cybersecurity agenda. Readers will be able to walk with the many stakeholders who participated in these annual EuroDIG discussions through the maze of cybersecurity challenges and opportunities. They will learn how the outcomes, recommendations and solutions, published in the concise terms of EuroDIG Messages, were reached based on consensus amongst the participating diversity of stakeholders.

Executive summary

The cybersecurity track at EuroDIG has developed and matured since the first forum was held in Strasbourg in 2008 according to the needs of stakeholders to scope the opportunities, challenges and problems. At times it was necessary to revisit some of the key issues and redefine them by bringing expert stakeholders together to examine the latest technology developments and assess their impacts on the evolution of the Internet and the digital revolution. This is why we can witness several phases in the development of the EuroDIG discussions, even though the transition from one stage to the next was never dramatic: it was a gradual evolution.

The first phase from the launch of EuroDIG until 2014 considered security issues in the context of the multistakeholder model but year by year one could witness the struggle of taking the discussion forward from "in which manner" (i.e. multi-stakeholder) to "how exactly" (i.e. what is the process). The discussions addressed many emerging issues including the exponential growth of new forms of cybercrime and what was needed to investigate and prosecute online crime effectively, the rapid development of borderless technologies such as cloud computing, the risks increasingly associated with the emerging social networks, and the protection online of fundamental human rights, privacy and security.

In the next phase in 2015 – 2017 the cybersecurity sessions developed a two-fold approach. Firstly, they continued to focus on scoping new challenges and identifying possible solutions. As cybersecurity inevitably moved up the list of priorities for governments, the stakeholder community became increasingly aware of the need to preserve and maintain the multi-stakeholder approach to addressing these critical issues.

A second no less important goal was to increase awareness amongst European Internet stakeholders of the growing complexity of the cybersecurity environment and the need to build and sustain trust in these transformative technologies. It became essential therefore to create the capacity for everyone to participate actively in these processes and provide inputs.

Enhancing the interactivity of stakeholder discussions, maximising inclusion and diversity, and strengthening the collation of inputs on cybersecurity issues became therefore increasingly important goals for EuroDIG's organising teams and their consultations with

stakeholders in preparation for the annual forum.

In the third phase in 2018 – 2020 the cybersecurity discussions moved from considering cybersecurity as an overarching problem, to building discussions around specific issues in the European context, such as the emergence of cyber norms, increasing user safety, and specific proposals to enhance the frameworks for cybercrime investigations. This was a further sign that the diverse EuroDIG community of stakeholders had established the facility to develop a common understanding in the complex field of cybersecurity.

The chronological overview of the sessions shows therefore that while cybersecurity has always been on EuroDIG's agenda, it has developed different dimensions in the context of what had emerged in successive years as specific new priorities. Thanks to the active participation of experts from all stakeholder communities, the EuroDIG forum has consistently demonstrated its capacity to scope, scrutinise and constructively discuss issues in an open and inclusive manner, and to draw conclusions, define concrete proposals and publish consensus-based recommendations as EuroDIG Messages for cascading to all Internet communities in Europe and worldwide.

The following chronological review of cybersecurity discussions and outcomes at the annual EuroDIG multistakeholder forum is covered in three parts:

- Part One
  EuroDIG 2008 – 2014: Reacting to the most pressing cybersecurity issues and creating a space for dialogue.
- Part Two
  EuroDIG 2015 – 2017: Cybersecurity as everybody's concern. Revisiting and rescoping the issue and getting stakeholders involved in the debate.
- Part Three
  EuroDIG 2018 – 2020: Global issues in the European context.

Part One

EuroDIG 2008 – 2014: Reacting to the most pressing cyber-security issues and creating a space for dialogue

Strasbourg 2008: Cybersecurity from a security, privacy and openness perspective

The issue of cybersecurity was a prominent theme on the agenda of the inaugural EuroDIG forum which was convened in Strasbourg in 2008. The first compilation of EuroDIG Messages reflected the common values shared by many European stakeholders, including trust, focus on multi-stakeholder process, and fundamental rights. Recognition of these values set the context for cybersecurity-related discussions at EuroDIG in the years ahead.

The 2008 programme included a session on European perspectives on fostering security, privacy and openness on the Internet. This discussed the interplay between these issues with the focus of minimising the trade-offs between them[2]. The discussions covered cybercrime-related aspects and the enhancement of legal frameworks in tackling the problem of online crime, without compromising privacy or the openness of the Internet. This would be a recurring theme of concern in subsequent EuroDIG discussions

It was clear from this first EuroDIG discussions that the issues of security, privacy, and openness on the Internet were best addressed in conjunction with each other. It was also noted that European policies concerning these issues "must be based on fundamental rights and the rule of law"[3]. The discussions in Strasbourg also highlighted the role of trust and co-operation between all stakeholders in tackling the problem of cybercrime.

Geneva 2009: The promise of public-private partnerships

Following the session on cybersecurity in 2008 which had considered the issues of security and privacy in the context of the open Internet, the session during the second EuroDIG forum in Geneva looked at cybersecurity and cybercrime from the perspective of cooperation between stakeholders primarily in industry and government administrations. This focus was consistent with the trend of growing support amongst many international organisations, governments, and non-governmental stakeholders for public-private partnerships as providing the most promising means of addressing the challenges of cybersecurity and the growing problem of online crime.

With regard to legislative approaches to tackle cybercrime, the concluding messages from the session encouraged stakeholders to follow the widely accepted approaches adopted in the Council of Europe's Convention on Cybercrime (the "Budapest Convention") rather than to develop competing legal frameworks[4].

The 2009 EuroDIG programme also included a workshop on specific aspects of cybersecurity and cybercrime. **Workshop 4: Cybercrime and cybersecurity: Private-Public Partnerships** aimed to identify the current challenges and emerging threats. As during the first EuroDIG forum, the session had a broad scope and tried to cover as many aspects of cybersecurity as possible including harmful online activity such as child abuse images, phishing, malware, botnets and illegal money flows on the Internet.

With regard to collaborative efforts to tackle cybercrime and provide greater cybersecurity, the workshop mainly focussed on the role of intermediaries. Participating stakeholders agreed that the way forward to build effective public-private partnerships was to address these issues on a national, regional and global level.[5] The discussion also acknowledged the crucial role of national and international legal frameworks such as the Budapest Convention in tackling cybercrime and data protection[6].

The session concluded that it might not always be possible to apply more widely regulatory and legislative interventions and cooperative approaches that worked in one particular context. For example, the success of mechanisms for cooperation with intermediaries in blocking child abuse websites did not mean that this approach would also work for other forms of harmful or illegal content. The workshop participants stressed that any col-

laborative interventions in the form of new multi-stakeholder models of regulation would require rigorous assessment as to whether they could address a particular problem as intended.

Madrid 2010: Cybercrime, jurisdiction, and cloud computing

The discussions on cybercrime continued at the third EuroDIG forum in 2010 in Vilnius. **Workshop 1: Cross-border cybercrime jurisdiction under cloud computing** focussed on the issues of transborder access to data, and industry initiatives and practices surrounding the jurisdictional aspects of cloud computing. The workshop aimed to raise awareness of this issue, to assess the suitability of various frameworks related to access to data stored in the cloud, and to suggest possible solutions for developing future policies in this area[7].

This discussion was quite timely: in 2010 the issue of investigating cybercrime and collecting electronic evidence solutions had become increasingly problematic for legislators, law enforcement agencies, and businesses, due to the growing adoption of cloud-based solutions. The issue of transborder access to data was also on the agenda of the Council of Europe in relation to the provisions of the Budapest Convention[8]. In addition to the jurisdictional aspects of the problem, the EuroDIG session also raised concerns relating to data retention frameworks which at that time were under scrutiny in the constitutional courts in Romania and Germany[9].

The workshop highlighted a number of problems related to access to data in the cloud for the purpose of pursuing criminal investigations. The first set of issues identified in particular by the representatives of law enforcement and the global IT companies (the so-called “big tech”) related to the increasing uncertainty of the application of legal frameworks for investigations, in particular the European Data Retention Directive (2006/24/EC), and related jurisdictional questions. EuroDIG provided a unique opportunity for these issues to be considered from different stakeholder perspectives through the participation of experts representing law enforcement agencies,

Internet service providers, civil society and industry, as well as noted academic experts[10].

The discussions recognised the existence of a legal quagmire for industry created by the absence of clear guidelines for transborder access to data. The EuroDIG Messages from the workshop called for further strengthening of international legal frameworks in order to gain more clarity, especially with regard to the criteria for law enforcement access to information stored in the cloud. It was also stressed that these frameworks should respect fundamental rights.

Another aspect stressed in the discussion and session outcomes was the need to further harmonise cybercrime legislation and provide increased training on cybersecurity issues for law enforcement agencies. Furthermore, this critically important workshop identified the potential role of public-private cooperation in efforts to build capacity and improve collaboration between industry and law enforcement[11].

> A representative from a big tech company in Workshop 1 emphasised the importance of the EU Stockholm Programme (2009) under the EU's Internal Security Strategy which included law enforcement cooperation mechanisms and proposed the creation of a new European cybercrime agency to tackle the problem of law enforcement access to data stored in the cloud. The speaker also referred to the new mandate for the European Union's Agency for Cybersecurity (ENISA) and expressed the hope that ENISA and the new cybercrime agency would work closely together[12].

The conclusions and EuroDIG Messages from the workshop recommended that the Council or Europe and the European Union should join with other international organisations in establishing a multi-stakeholder working group comprising experts from the private sector, civil society, academia, and government policymakers in order to develop guidance on the issues related to access to data in cloud computing. The proposed areas of focus of this guidance would be cybercrime investigations, data protection, jurisdiction, and legal conflicts.

The workshop also recommended in its messages that the Council of Europe should consider drafting specific policies and guidelines for law enforcement on trans-border investigations[13].

Belgrade 2011: Exploring the landscape of cybersecurity and emerging threats of cybercrime

The issues of cybersecurity and cybercrime were separated in the agenda of EuroDIG 2011 in Belgrade as two different aspects of security-related issues. While the second main plenary discussed the broader aspects of cybersecurity, Workshop 7 in the programme focussed on cybercrime and the new threats posed by social networking websites[14].

Plenary Session 2: Cybersecurity: Cleaning-up businesses and infrastructures opened with a discussion about the differences between cybersecurity and cybercrime in order to put cybersecurity in the broader context of online threats and to identify different regulatory levels required to address challenges such as critical infrastructure resilience, emergency responses, and information sharing. The session also touched upon problems that small and medium-sized enterprises (SMEs) face in addressing cybersecurity threats. Representatives from governments and industry spoke in support of raising awareness amongst SMEs about cybersecurity and involving them in the processes for addressing current threats[15].

One of the contentious issues raised by civil society and youth participants was the risk of the financial interests of private stakeholders potentially subordinating and undermining the public interest goals in cybersecurity[16]. Speakers from academia, not-for-profit organisations and the European Commission also highlighted that while cybersecurity was a strong public interest concern, it should be taken into account that private businesses run and manage ICT infrastructure. It was not possible to develop effective policies to counter cybersecurity threats in a top-down manner due to the lack of instruments to enforce such policies[17].

The concluding EuroDIG Messages from the plenary session made clear that while experts in the industry who were running networks provided the technical responses and solutions, cybersecurity threats could not be left to the private sector to deal with due to the strong public interest aspects of the problem. Furthermore, there was an acknowledgement that cybersecurity issues should not be delegated solely to governments and regulatory authorities[18].

There was broad agreement that traditional top-down command-and-control approach-

es to regulation had failed to develop long term solutions to cybersecurity threats. Rather there was a need for 1. meaningful consultation between governments, regulators and stakeholders in the private sector; and 2. effective awareness-raising amongst all parties, including end-users, in order to ensure a balanced approach to assessing risks and opportunities. EuroDIG was seen as one of the important multistakeholder for a which facilitated this[19].

EuroDIG's workshop on cybersecurity in Belgrade – **Workshop 7: Cybercrime and social networking sites. A new threat?** – discussed the growing popularity of social networking websites where it was noted that users (including children) were encouraged to share significant amounts of personal information about themselves. It also reviewed the opportunities that social networks created for malicious actors who used these platforms for collecting personal data[20], identity theft and copyright violations.

The workshop concluded that there was a need for active redress mechanisms which users of social networks could utilise across borders both within Europe and globally. It was emphasised that the current lack of awareness amongst children and adults about the security and privacy threats of social networking was a major concern. There was a need to empower users of all ages in order that they could protect their interests when engaging in social media websites[21].

Stockholm 2012: Feasibility of public-private partnerships in tackling cybercrime and safeguarding cybersecurity

The cybersecurity session at EuroDIG 2012 in Stockholm brought the issues of cybercrime and cybersecurity together again in **Plenary Session 5: Public-private cooperation in the fight against cyber-crime and safeguarding cyber security?** The session reviewed examples of national and international initiatives aimed at addressing various cybersecurity and cybercrime issues, including illegal content, infrastructure resilience and the whole lifecycle of cybersecurity. These included the Clean IT Project initiated by the EU, the Global Net-

work Initiative (GNI) – an alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions projects run at the national level in Serbia and Sweden, the Centre for the Protection of the National Infrastructure (CPNI) in the UK, and ENISA's European Public-Private Partnership for Resilience (EP3R)[22].

The Plenary discussion focussed on the various challenges that these partnerships faced. The participants first of all examined the drawbacks of reporting and blocking illegal content with the help of private industry. There was broad recognition of the need to tackle the root of the problem i.e. illegal activity online, in addition to action to block access to particular types of content[23]. This led to a discussion about the risks of "over-blocking" and the measures that had to be taken by both public and private partners to prevent incorrect blocking and ensure there was no gradual increase in the scope of content blocking.

Secondly, questions were raised about lack of transparency and adequate safeguards for the protection of human rights, adherence to due process and respect for the rule of law. The benefits of independent oversight were also considered[24].

The Plenary's panel of experts emphasised the challenges for cooperation between law enforcement and private sector entities when tackling and investigating cybercrime offences. It was pointed out that law enforcement and private companies had different accountability regimes.

The session's conclusions and messages emphasised that self-regulation did not place online content providers above the law; they had to follow due process mechanisms, transparency, accountability and respect for human rights when implementing and enforcing self-regulatory frameworks[25].

Lisbon 2013: Multistakeholder models in cybercrime and cybersecurity

EuroDIG in 2013 held in Lisbon took place in the immediate aftermath of the Snowden revelations of alleged global surveillance programmes. This had an impact on the cybersecurity and cybercrime discussions and access to data and trust were issues high on the EuroDIG agenda. Both cybersecurity sessions – **Plenary Session 5: Multistakeholder approach to fighting Cybercrime and safeguarding Cybersecurity** and **Workshop 6: Security as a multistakeholder model** – focussed on framing responses to online crime and security within the multistakeholder perspective[26].

Plenary Session 5 discussed the role of intermediaries and other stakeholders in cybercrime investigations and in the broader context of safeguarding security in cyberspace. The main points of disagreement in the discussions concerned the different perspectives that representatives from the ISP industry, law enforcement agencies, and civil society concerning the validity of law enforcement requests, the effectiveness of mutual legal assistance mechanisms, and respect for due process. The session also discussed possible conflicting approaches to the development of legal frameworks for cybersecurity and cybercrime, such as Council of Europe conventions and initiatives led by the International Telecommunication Union (ITU) and the UN Office on Drugs and Crime (UNODC)[27].

The session participants acknowledged that while traditional cooperation methods of cybercrime investigation tended to fail, there was a need to ensure that cooperation between law enforcement and industry adhered to the rule of law and due process.

> A government representative and a panellist from the ISP industry highlighted the approaches of the Council of Europe to facilitate cooperation between ISPs and law enforcement and to involve various stakeholders in this process. The ISP representative expressed the opinion that these inclusive approaches could be more effective in terms of human rights, safeguards, and multistakeholder involvement, than directives coming from the governments and international organisations[28].

> An issue raised by a representative of the technical community concerned broader stakeholder cooperation helping to shift the focus from the differing objectives of governmental agencies and other stakeholders, in order to identify problems and find solutions.
>
> Another participant stressed the need to be careful that discussions about cybersecurity and cybercrime frameworks did not become a situation of "us against them," i.e. law enforcement against the ISPs[29].

Further discussion in the Plenary Session highlighted how managing multiple risks in cyberspace was normally the responsibility of more than one actor, and that shared responsibility was consistent with the characteristics of global information networks.

The Plenary Session acknowledged the importance of trust not only between public and private parties but between users and providers, and the trust of citizens generally in communications services. It was important in this context to establish safeguards that ensured the right balance was maintained between the need for government and law enforcement interventions for the purposes of protecting and enhancing cybersecurity, and data privacy protection[30].

This question of balancing trust and due process was also a prominent concern in the discussions at EuroDIG about transborder access to data. Given the growing number of requests from law enforcement agencies located in another country, the representatives of the technical community and "big tech" expressed the view that trust between intermediaries and law enforcement required the provision of effective mechanisms for the verification of such requests, adherence to due process, and maximising transparency and accountability.

The Plenary Session also discussed the problems of intermediaries who increasingly found themselves having to balance the need to retain the trust of users and the requirements of law enforcement agencies. Many participants in the session expressed the fear that the loss of the trust of either risked eroding the fundamental nature of the Internet[31].

The EuroDIG workshop on cybersecurity – **Workshop 6: Security as a multistakeholder model** – covered various aspects of cybersecurity, taking into account that the Internet had become both a key infrastructure for communications and a major platform for social, political and economic activities. Cybersecurity was seen as a shared responsibility: the involvement of all stakeholders from the differ-

ing sets of stakeholders and sectors was therefore crucial, including IT hardware manufacturers, the financial sector, the Internet's technical community and Internet service providers.

The workshop discussed the need for a commonly agreed definition and shared understanding of cybersecurity and of "multistakeholderism". The workshop participants who represented various stakeholder groups agreed several key aspects, including transparency, cooperation, engagement, information sharing and collective learning[32].

The workshop discussions also highlighted the views of many participants that the traditional approaches to law and regulation when applied to activities online tended to go in the direction of greater control, monitoring of citizens' behaviour and compliance, thereby producing even more regulation and enforcement. Based on the opinions expressed in the discussion, there was a call for smart regulation that included problem-oriented solutions based on cooperation between stakeholders[33].

The conclusions and EuroDIG Messages drawn from the workshop recommended that governments could act as facilitators, providing incentives and encouraging dialogue between these various stakeholder groups, contributing support for capacity building and increasing the inclusion of cybersecurity in educational curricula. The session outcomes also highlighted the need for a balanced approach to security concerning the necessity of safeguards and respect for due process and fundamental rights[34].

Berlin 2014: Fundamental rights and the rule of law in focus

There were two Plenary Sessions during the 2014 EuroDIG event held in Berlin. **Plenary Session 5: Security, Internet principles and human rights** debated the notion of security and considered how the term could be misused and abused by state authorities to justify interference with the fundamental rights of citizens. Taking into account the definition of security from different stakeholder perspectives and various historical and political contexts, the session's report highlighted how the definitions of terms such as *"national security"*

and *"terrorism"* often remained vague, and that certain governments cited threats to national security as justifying responses such as mass surveillance of citizens' online activities[35].

The G20 Plenary discussion concluded by acknowledging the need to re-conceptualise Internet security so that it included the core values of human rights. The report of the Plenary called for efforts to find the right balance between the protection of human rights-based freedoms and security in the heterogeneous world of morals, values and ideals.

The session's conclusions and EuroDIG Messages underlined that the Internet was a tool for communities to defend their rights against undemocratic governmental and social repression: in other words, the Internet *"should not allow Big Brother to watch us but should allow us to watch Big Brother"*[36].

Plenary Session 6: A secure and non-fragmented cyberspace: rule of law in a cross-border environment took forward the discussions originally held in the EuroDIG Plenary on cybersecurity and cybercrime in 2013 and considered issues relating to the rule of law in a cross-border environment. The session considered the issue of possible fragmentation of legal approaches and reviewed ways to avoid conflicting legal frameworks.

Another aspect raised in the Plenary discussion was whether differences in legal frameworks could contribute to technical fragmentation of the Internet where access to content was blocked in one country because it was illegal under its national law. However, some participants in the Plenary session believed this was unlikely[37].

Speakers from the Council of Europe, the ISP industry and academia expressed an opinion, which was supported by the audience at the end of the session, that the Council of Europe's Convention on Cybercrime was potentially a good basis to avoid legal conflicts and to harmonise legislation. It was generally agreed that the framework provided by the Convention could be a starting point for agreeing global multi-stakeholder commitments on tackling the problem of cybercrime[38].

The session also discussed the issue of collaboration between industry and governments in tackling cybercrime, with a particular focus on the role of ISPs in this ecosystem and extending that from being solely a conduit that provided data in criminal investigations, to include protecting users from spam, malware etc. The role of other intermediaries including the social media platforms was also considered[39].

These discussions revealed that some international legal frameworks for removing illegal

content had not been developed based on wide support and consensus. The representatives from the Council of Europe, the ISP industry and some members of the audience highlighted the problems related to these disparities. The members of the session's panel agreed that this was an issue of possible disagreement in the area of harmonisation of legal frameworks[40].

The final EuroDIG Messages from this session acknowledged that some issues such as illegal content might lack the necessary legal instruments for harmonisation of approaches. The session members called for all stakeholders to work together to handle these issues when national legal frameworks differed significantly[41].

Part Two

EuroDIG 2015 – 2017: Cybersecurity as everybody's concern. Revisiting and rescoping the issue and getting stakeholders involved in the debate

Sofia 2015: Cybersecurity discussions as a way to build stakeholders' capacity

The organising team of the cybersecurity sessions at EuroDIG in 2015 held in Sofia decided to shift the approach to cybersecurity issues towards building the capacity of the EuroDIG stakeholder community to participate in related discussions. Recognising the complexity of the challenge of tackling cybersecurity threats, the cybersecurity workshop and its follow-up session had two aims. The first was to engage everyone in the cybersecurity discussion; the second was to cluster cybersecurity issues and discuss where and how they were addressed, with the overall goal of identifying actions that stakeholders should take to mitigate and resolve cybersecurity problems[42].

Workshop 5 and its follow-up session under the heading **Cybersecurity: bringing the puzzle together** was structured as an interactive workshop that opened by inviting the audience to explain their concerns related to cybersecurity. These were clustered under various headings including international peace and security, cybercrime, critical resources and protection of children in the digital age. The second part of the session focussed on discussing the over-arching theme of who should take responsibility for address the cybersecurity issues raised in the first part.

While recognising the necessity for cooperation and the ongoing efforts of governments and industry to provide and maintain cybersecurity, the discussion in the workshop emphasised the need to take into account the distinct mandates of certain stakeholders, such as the

unique role of the governments in law-making and law enforcement. The discussions emphasised the need for clear and transparent frameworks outlining who decided what was right and what was wrong when it came to the law, regulation and enforcement[43].

The discussions also highlighted the difficulties in finding the right balance between governmental interventions and voluntary approaches in the cybersecurity ecosystem due to the fast-evolving nature of cyber-threats, the complexity of regulatory domains, and the many actors involved in cybersecurity.

The workshop also reflected on the so-called "cybersecurity divide" in Europe regarding the capacity of governments, industry, and law enforcement agencies to address the complexities of establishing and maintaining an adequate level of cybersecurity. The workshop participants recommended that the current fora for multi-stakeholder discussions which brought together government policymakers, law enforcement agencies and non-government stakeholders should strengthen their process of dialogue and increase stakeholder inclusion.

The workshop discussions endorsed the following fundamental aspects of cybersecurity: education, cooperation, building and restoring trust, and protection of fundamental rights online[44]. A key conclusion in the session's contribution to EuroDIG's Messages was that governments and regulators should undertake assessments of the impacts of regulatory intervention and enforcement in order not to inhibit innovation and constrain the development of new technologies[45]. Session participants recognised that cybersecurity required on the one hand robust frameworks of criminal law and procedure, safeguards and human rights protection measures, and on the other hand flexible regulatory responses and measures for building trust[46].

Brussels 2016: Cybersecurity practices and how to bring them from state of play to state of art

Building on the success of the interactive dialogue held during the previous year's EuroDIG forum, the cybersecurity workshop during EuroDIG in 2016 in Brussels moved the focus from mapping cybersecurity issues to the question of how these issues were addressed in Europe.

Workshop 5: Cybersecurity revisited, or are best practices really best? was another highly interactive EuroDIG session which discussed the progress of on-going multistakeholder and multilateral processes such as the UN Group of Government Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), the Council of Europe's Cloud Evidence Group which explored solutions for criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions (including through mutual legal assistance), and the Global Forum on Cyber Expertise (GFCE), a multistakeholder community that promoted international collaboration in capacity building.

The first part of the session focussed on best practices in cybersecurity and examined whether they were indeed the best and what might be done to improve these practices. The session identified several concerns. The most important according to civil society representatives concerned openness and participation. Multistakeholder processes provided the best way to achieve workable solutions because they enabled expert stakeholders at an early stage in the process to identify, discuss, and address possible drawbacks and flaws in proposals for conventions, legal frameworks and regulation. It was especially important for civil society representatives to be able to ensure the inclusion of fundamental rights and freedoms in cybersecurity proposals and ensure that these were reinforced rather than undermined by new cybersecurity proposals.

While multilateral cybersecurity processes led by governments were becoming increasingly open for multistakeholder inputs, it was often the case, however, that the final negotiations took place without the direct participation of civil society and business representatives. Intergovernmental processes lacking such openness and transparency risked eroding the trust of citizens and Internet users in the role of governments[47].

> One civil society representative expressed the view in Workshop 5 that negotiations of cybersecurity frameworks often considered human rights and security as a dichotomy of opposing positions that led to decisions in favour of one over the other. However, it was equally important for cybersecurity policies to reinforced human rights[48].

The follow-up discussion to Workshop 5 under the heading **The future of cybersecurity in Europe – from state of play to state of art**, opened by taking forward the earlier discussion on best practices with the aim of making specific recommendations for improvements. Participants raised the issues of building trust and considering cybersecurity as a process and not a result. The discussion highlighted that security can relate to both security of tools and security of processes. The debate emphasised that openness and trust were equally important for both aspects[49].

Further discussion focussed on trust as a necessary prerequisite for providing cybersecurity. There were various perspectives of trust: trust between institutions, the trust of end-users in products, user trust in the Internet. The session considered whether these various aspects and manifestations of trust could be mutually reinforcing. It was generally agreed that governments could be considered as a channel for building user trust because they could legislate with this aim in mind. It was usually the private sector, however, that had the critical role of implementing these legal requirements s that they became effective.

It was also noted that cybersecurity regulations normally set the obligations on providers at the end of the value chain, such as the telecommunications operators, and not on the vendors or companies that produced and supplied end-user equipment. This was due to the complexity of the global supply market and inability to enforce regulation or promote better practices at the start of the chain[50].

The session agreed several conclusions for inclusion in EuroDIG Messages relating to improvement of best practices and the way forward in building trust[51].

Firstly, it was important to broaden cooperation on cybersecurity by bringing stakeholder communities closer together to help them learn from each other's good practices. It was emphasised that good practices always included the creation of trust between the different parties involved. For example, the development of practices for tackling the problem of spam had been largely achieved through cooperation between community emergency response teams (CERTs) and law enforcement agencies.

The workshop's conclusions also recorded that there was general agreement about the existence of a gap between the diplomatic and military communities on the one hand, and the technical communities on the other when framing cybersecurity proposals. Differences in the discussions risked creating fundamental misunderstandings and both communities were urged to continue open and inclusive dialogue.

Finally, the session outcomes acknowledged there was a need to bring together the multitude of platforms and initiatives working on cybersecurity, especially in the field of capacity building, in order to promote collaboration and avoid duplication of efforts. The participants in the EuroDIG session underlined the necessity to make these initiatives and processes more open, transparent and inclusive with the active participation throughout of the various stakeholders with a major interest in cybersecurity.

Tallinn 2017: The growing importance of governments' role in cybersecurity

EuroDIG 2017 in Tallinn had several sessions devoted to cybersecurity. In addition to a Plenary Session on mapping the cybersecurity landscape in Europe and beyond, there were two workshops on multi-stakeholder approaches to cybersecurity, and on criminal justice in cyberspace. In addition, the technical community organised an educational track session about the technical realities behind the headlines.

The opening Plenary Session **Alice in Wonderland – mapping the cyber-security landscape in Europe and beyond** explored changes in the cybersecurity landscape in Europe and discussed how these influenced the perceptions and actions of different stakeholders[52]. The session marked one of the fundamental changes in EuroDIG's discourse on cybersecurity by examining the leading role of governments in cybersecurity, especially with

regard to national policies and regulations, co-operation with other stakeholders, cross-border cooperation, and the development of norms for responsible state behaviour in cyberspace.

The role of governments was framed in the discussion from different perspectives: consumer protection; the security of citizens; the emerging regulation of the Internet of Things (IoT); and protection of critical infrastructure.

> The importance of the EU's Directive on Network and Information Systems (NIS) for the protection of essential services and critical infrastructures was highlighted in the Plenary Session by a representative from the technical community as providing financial incentives for businesses to invest in protecting society from cybersecurity threats. It was also pointed out by other participants in the session that in addition to the adoption of regulatory frameworks, there were increasing calls for norms to be agreed relating to responsible behaviour of state and non-state actors in cyberspace[53].
>
> While recognising that governments played a unique and growing role in providing cybersecurity, especially through creating and enforcing rules and regulations, there were expressions of concern by representatives of the technical community that some governments lacked sufficient technical expertise or were driven by political agendas and a desire to control citizens' online behaviour and activities.
>
> Some participants from the technical community expressed the view that government policies could result in a variety of approaches at the national level. For example, some governments defined critical infrastructure while others did not. For private stakeholders operating across borders this kind of inconsistency in governments approaches to national policy created additional complexity and lack of clarity as to who was responsible for a particular part of the national infrastructure[54].

Stakeholder participation in the development of cybersecurity policies was highlighted as crucial to provide the necessary expertise, to ensure transparency, and to hold public authorities to account. This was reflected in the conclusions and the EuroDIG Messages[55].

The workshop on cybersecurity issues in the EuroDIG programme in Tallinn – **Workshop 9: Stress testing the multistakeholder model in cybersecurity** – discussed collaborative security models as a different kind of multistakeholder approach[56]. Based on the outcomes of the Plenary 1 session which had mapped the

cybersecurity landscape, the workshop also took into account opinions as to whether governments always had a leading role in cybersecurity.

The different roles that stakeholders had in implementing regulations and laws was also discussed. It was generally acknowledged that while aspirations always expressed support for public-private partnerships and multistakeholder collaboration, the complexity of the cybersecurity environment created a lack of understanding of what „multistakeholder" meant in practice and what the various roles and responsibilities of stakeholders were.

The workshop also discussed the various incentives, economic reasoning and interests of cybersecurity stakeholder communities.

While recognising that governments could take a leading role in developing cybersecurity policies, it was generally agreed that the processes for developing these policies should be multistakeholder. In this regard, it was stressed that civil society participation was vitally important as their involvement helped to ensure greater transparency and accountability in the final proposals. The EuroDIG Messages from the workshop recommended accordingly that collaborative multistakeholder approaches were the best way to bridge these differing perspectives amongst the stakeholder community[57]. Furthermore, taking into account how the Internet was constituted and how it worked, the workshop concluded that each party had a responsibility to foster resilience and to adopt a collaborative approach to addressing cybersecurity that promoted confidence and supported social and economic opportunities[58].

Workshop 4 in the EuroDIG programme under the heading **Criminal justice on the Internet – identifying common solutions** approached the issue of cybercrime from a broader perspective. With most online criminal activity leaving digital traces, the organising team considered it important to change the discourse and examine the emerging challenges of pursuing criminal justice on the Internet and obtaining electronic evidence. The workshop aimed to ensure that the various stakeholders involved in criminal investigations were aware of each other's problems and cooperating in the search for common solutions[59].

Participants in the workshop discussed the significant problem of digital evidence collection and the lack of systemic approaches at that time. In the absence of effective legal frameworks ad hoc solutions such as voluntary agreements between industry and law enforcement were considered to be ineffective in addressing what had been described as the

lawless "Wild West of the Internet." The participants called instead for structured solutions including modification and harmonisation of existing legal standards for digital evidence collection, standardisation of request forms, capacity building and training in the law enforcement community, and the establishment of channels for facilitating requests such as online portals. The work of the European Commission in this area was also discussed as potentially providing better tools for cooperation with Internet service providers (ISPs), within the EU and externally, in order to obtain access to digital evidence[60].

The workshop's concluding EuroDIG Messages emphasised the need for safeguards and human rights to be included in frameworks for online criminal investigation, and for transparency in the process of developing new solutions and related procedures. It was also recommended that all stakeholders should be involved in the processes for the development of these solutions.

The workshop participants also agreed that there should be an increase in the capacity of law enforcement agencies to process requests for data access in criminal investigations. At the operational level, law enforcement and Internet intermediaries had to create a better shared understanding of the reasons behind the request for digital evidence[61].

With regard to specific technologies, the workshop discussed the use of the Carrier-Grade NAT or LSNAT (large scale network address translation) standard. Representatives of law enforcement and the technical community considered its use to be a contentious issue for cooperation in criminal investigations[62]. The workshop's EuroDIG Message on this issue called for better engagement between law enforcement agencies and the Internet industry in reducing the use of technologies that prevented attribution in criminal investigations[63].

Part Three
EuroDIG 2018 – 2020: Global issues in the European context

Cybersecurity discussions at EuroDIG reached a turning point in 2018 when the focus shifted from discussing general issues of cybersecurity to specific topics identified by stakeholders in the call for issues during the preparatory phase.

Tbilisi 2018: Cybersecurity and emerging challenges for non-state actors

Cybersecurity discussions during the 2018 EuroDIG forum in Tbilisi focussed on two specific issues that were high on the agenda of various stakeholders:

1. the role of non-state actors in setting norms of responsible behaviour in cyberspace. This stemmed from the trend of private sector entities coming forward with proposals for international instruments for responsible behaviour in cyberspace, notably Microsoft's Digital Geneva Convention to protect cyberspace. The key issue was whether private sector entities had the authority and legitimacy to make such proposals[64].
2. the cross-cutting issue of economic opportunities and security challenges of the Internet of Things (IoT)[65]. This was not a new area of focus for EuroDIG but it was high on the agenda of cybersecurity policymakers in the EU at this time, in particular the European Union Agency for Cybersecurity (ENISA), as well as industry and research communities.

Workshop 9 in the EuroDIG programme under the heading **Non-state actors in Europe and beyond: The true shapers of cybersecurity norms?** discussed the role of non-state stakeholders in the various emerging international

cybersecurity norms development processes. It approached the topic from the general position of non-binding norms as an appropriate tool for governments in international relations and providing stability and security in Europe. The workshop then proceeded to discuss policymaking by non-state actors in the field of international cybersecurity policymaking and the possible implications for both state and non-state stakeholders. The session examined how non-state actors in Europe and other regions had become involved in such voluntary norm-making processes – as opposed to international rules based in law – and the strategies they had employed.

The risk that strong regulation of cyberspace would stifle innovation and development was also considered. The workshop participants generally agreed that there was a disconnect between new technologies and the responses of governments and regulators and that norms created by industry as a form of self-regulation might potentially serve as a starting point for building norms for agreement at the international level[66].

> It was pointed out by representatives from governments, the telecoms industry and civil society that states had made great progress in negotiating principles for cyberspace regulation. This was despite some notable failures, such as the inability of the UN GGE (Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace) to reach consensus in 2017.

Workshop participants acknowledged that there were problems concerning the development of norms and principles generally and the ability of non-state actors to play an effective role in these processes. Key concern included:

1. the differing political context that might frame the norms and principle – e.g. 'western principles' vs. 'eastern principles';
2. transnational private industry players seeking to develop their own international norms for governing behaviour in cyberspace and then submitting these proposals for endorsement. Industry players inevitably sought to advance their own interests in the norm-making process, with reference to their commercial objectives in the development of markets.

It was generally agreed in the workshop that non-state entities should not be able to dictate the content of international conventions for cyberspace because it remained the responsibility of states to agree legally- binding norms[67]. It was also recognised that civil society performed a valuable role in promoting the

involvement of industry in the largely multilateral processes to develop norms of behaviour, instead of producing their own separate initiatives[68].

It was recognised in the workshop's conclusions and contribution to EuroDIG's Messages that cyberspace would inevitably be subject to political involvement due to the perception of the so-called "cybersecurity arms race." However, the workshop participants agreed that framing the debate as "cyberstability" rather than as "cyberwar" would provide more opportunities for all stakeholders to contribute to the drafting of rules that would ensure the development of a more secure global information society and digital economy. This recommendation came with an acknowledgement that all stakeholders were responsible for their actions in cyberspace[69].

The workshop on cybersecurity held in Tbilisi – **Workshop 5: IoT – economic opportunities and security challenges** – discussed recommendations for enhancing the security of Internet of Things (IoT) from three perspectives: the end user, policymakers, and industry. The workshop participants were split into three groups with each group discussing particular perspectives and tasked with producing related recommendations. The workshop agreed the following conclusions[70] which were reflected in the EuroDIG Messages[71]:

- Security standards embedded in IoT devices made them expensive; manufacturers currently lacked the incentives to adopt them because they reduced their commercial viability.
- Information about the security and safety of connected devices had to be clear, objective and easily understood.
- Whether through informal mechanisms or certification, users wanted the security of devices to be tested and officially verified.
- The security and safety of devices designed for children was a particular concern for consumers.
- Governments should engage with businesses and citizens in IoT research and development in order to ensure that public policy issues were taken into account.

In addition to the workshop sessions, the Council of Europe organised an information "flash" session in Tbilisi (No.13) under the heading **Challenges of cybercrime and transborder investigations**. The session focussed on access to data, standards, public-private partnerships and the "follow the money" approach to investigating online criminal proceeds[72].

The Hague 2019: Cybersecurity, peace, and justice

EuroDIG 2019 held in The Hague had the largest number of cybersecurity sessions in the forum's history[73]. This was perhaps not surprising in "The City of International Peace and Justice" and The Netherlands had been among the leaders in Europe in setting the agenda for cybersecurity, especially concerning collaborative approaches.

Based on the topics for discussion submitted during the preparatory call for issues, the main EuroDIG event agenda contained three cybersecurity sessions: a plenary on cyber norms and two workshops on 1. addressing technology challenges in cybersecurity and 2. criminal justice in cyberspace. Furthermore, a "day zero" pre-event was organised the Global Commission on the Stability of Cyberspace (GCSC) when stakeholder inputs on its cybersecurity recommendations were invited.

In addition, EuroDIG stakeholders organised two cybersecurity-related informational "flash" sessions on 1. the role of the governments in coordinated security vulnerability disclosures; and 2. a proposal to reconsider the key concepts of cybersecurity in the realm of growing concerns related to survivability.

Plenary Session 4: Making norms work – Pursuing effective cybersecurity considered the understanding of norms and their nature, multilateral norm-making processes, and the effectiveness of current norms. It was pointed out that multilateral processes led by governments relating to cybersecurity norms were becoming more open to multistakeholder inputs. It was recommended that this process of opening up these negotiations should continue and that so-called "swing states" should be convinced of the value of allowing more stakeholder participation. Speakers from differing stakeholder groups specifically highlighted the valuable roles and contributions of the technical community and civil society in these processes.

An interactive poll of the audience conducted during the session showed that the then current agreed norms had not been perceived as effective[74] and therefore the session's EuroDIG Messages suggested more effort was needed to develop norms on responsible state behaviour in cyberspace. The session's overall conclusion was that the development and implementation of norms needed to be done in an interdisciplinary way, and that these norms should be non-binding. The EuroDIG Messages recommended that multistakeholder and multilateral mechanisms should not be consid-

ered as ideologically opposing frameworks for agreeing norms but should be brought together[75].

> Some session participants expressed the view that the effectiveness of norms lay in their "like-mindedness" and cited the European Union as an example of an effective regulator and norm-maker because it brought together states with shared values[76]. Nevertheless, the session concluded in its Messages that while regional efforts were important, the Internet was global and there was a need for global solutions.

Workshop 7: Cybersecurity challenges ahead! How would you shape regulation to address changing technology? discussed how regulation needed to keep in step with the emerging technical challenges of the next decade. The EU intended to strengthen its approach through more cyber-related regulation amidst a growing global appetite for further regulation in the field of cybersecurity.

The workshop included in its conclusions and EuroDIG Messages a call for greater flexibility in determining whether further regulation was needed in every case. It also warned that a false dichotomy of "privacy vs. security" could significantly hamper the regulatory policymaking process and that support for security and privacy by design could provide the solution to this problem[77].

With regard to the development of regulatory frameworks, the workshop recommended that effective decisions could only be made if all the stakeholders' perspectives were taken into account[78] and emphasised that all relevant stakeholders needed to be at the table. It was acknowledged that some issues had to be settled by specific stakeholder groups with the required expertise. The workshop also concluded that there was a pressing need for national regulators to consider and implement stronger enforcement mechanisms.

Furthermore, in the absence of an independent judiciary for cyberspace, the session messages called for new mechanisms for dispute resolution that would complement existing legal frameworks.

Taking forward the debate in the Plenary Session when the role of like-minded countries was linked to the effectiveness of cyber norms, participants in the workshop suggested that the implementation of best practices by like-minded states could further strengthen the adoption of responsible behaviour by a larger number of actors[79]. The workshop also recommended:

1. increased transparency and more effective accountability mechanisms when address-

ing the challenges posed by emerging technologies.
2. digital literacy and consumer awareness about cybersecurity needed to be better implemented for a more effective holistic approach in combatting cyber threats[80].

Workshop 11 under the heading **Criminal justice in cyberspace – more of everything?** examined aspects of criminal justice in cyberspace from the perspective of applicable regulations, transborder access to electronic evidence and human rights, public-private cooperation and technical aspects of investigations[81]. The discussion in the workshop was triggered by recent European Union and Council of Europe initiatives that addressed the issues of greater cooperation for tackling cybercrime and cross-border requests for electronic data in criminal investigations. This reflected in particular the ongoing discussions at that time about the EU's e-evidence proposals.

Representatives from civil society, private industry, and law enforcement expressed several key concerns as to whether the EU proposals provided enough protection of fundamental rights, whether they took into account the different legal regimes of accountability of governments and private industry, and whether they provided sufficient safeguards against abuse.

It was apparent in the workshop that there were divergent views in particular among the private sector stakeholders on what kinds of frameworks were needed and how private industry would handle law enforcement requests for e-evidence[82]. The session was unable therefore to produce consensus-based recommendations on the EU's e-evidence proposals. However, the participants were able to agree the following conclusions and to feed into EuroDIG's Messages:

1. criminal justice instruments to contain safeguards and to ensure that fundamental principles were respected, including principles of proportionality, necessity and legality;
2. the need for increasing digital literacy in the law enforcement agencies, judiciary, and telecoms operators;
3. the importance of ensuring the Second Draft Protocol to the Council of Europe's Budapest Convention on Cybercrime worked for everyone, including non-EU countries, and the need for conditions, safeguards, and notifications to be present in the negotiated document[83].

Virtual 2020: The pressure of global cybersecurity challenges

In 2020, like many events around the globe, EuroDIG which had been scheduled to be held in Katowice became a virtual forum as a consequence of the COVID-19 pandemic. The European Internet governance community was able to respond quickly to the challenges of moving the forum online with a virtual format (if Internet governance events cannot be held successfully on the Internet, what could be?!). As the extensive social and economic lockdowns imposed in many European countries accelerated the transition online of almost every aspect of daily life and activity, inevitably EuroDIG's cybersecurity discussions needed to address the cybersecurity and online safety aspects and impacts of the global pandemic.

> In a EuroDIG pre-event some stakeholders organised an informal "birds-of-a-feather" session under the heading *COVID-19 pandemic – lessons learned for children's safety*[84] which set the scene for the cybersecurity sessions in the main EuroDIG programme covering the aspects of cybersecurity which had been brought into sharp relief by the pandemic: user confidence in cyberspace; the next challenges for criminal justice; and the impact of domain name system encryption on the Internet ecosystem and its users[85].

Workshop 2: Enhancing users' confidence in cyberspace – risks and solutions aimed to identify the challenges in addressing risks including the COVID-19 pandemic crisis. The discussion also explored solutions for ensuring user confidence and trust online[86]. With regard to addressing increased concerns about online security during the global pandemic crisis, it was agreed there was a need for stronger digital literacy, particularly for children, their parents and teachers, and citizens for whom the pandemic had made it a necessity to become part of the digital society, including the elderly. Workshop participants also generally agreed that digital literacy should be approached in an interdisciplinary manner.

The conclusions and EuroDIG's Messages also reflected the consensus in the workshop that users needed to become more aware of risks and be taught to think critically and differentiate between safe and unsafe practices[87].

The workshop also called for more user-friendly security provisions in devices and applications, an issue which was highlighted by

civil society and business sector participants. It was recommended that ICT providers needed to ensure greater transparency in their practices, especially regarding implementation of security by design and security by default principles in the development of their products.

Furthermore, the workshop participants recommended that manufacturers and suppliers should raise users' trust in their products through more transparency with regard to data management, handling of users' personal data, vulnerability disclosure and procedures for reporting inappropriate content on social media platforms[88].

Workshop 3: The Impact of DNS Encryption on the Internet Ecosystem and its Users focussed on the issues surrounding the adoption of DNS over HTTPS (known as DoH), a technical protocol which uses an encrypted connection for enhancing security when communicating with the domain name server. The main aspects discussed were 1. the effect of some models of DoH on the centralisation of the Internet's infrastructure that could potentially affect cybersecurity[89]; and 2. the different effects of encryption relating domain name system queries for end-users, Internet service providers (ISPs), operating systems, browsers, and applications.

The workshop participants from the technical community and the telecoms industry acknowledged that while the DoH standard recently published by the Internet Engineering Task Force (IETF) could result in stronger privacy and security for the end-user, there was a risk it could also create additional problems such as limiting the choice of DNS resolvers and operating system configurations. The discussion also pointed out the additional problems that DoH created for ISPs due in effect to its breaking the balance of power between the browser and operator communities and as a result creating potentially higher risks of market and network centralisation[90].

The workshop recommended in its conclusions and the EuroDIG Messages that the community should work on deployment models that would address these concerns, bearing in mind the need to educate end-users about how the domain name system operated and to increase the level of trust in ISPs and domain name resolvers. The conclusions also highlighted the need to consider legal aspects of the relationships between end-users and DoH/DoT providers[91].

Following the discussions about the challenges of cross-border access to digital evidence during previous EuroDIG discussions, **Workshop 7** under the heading **Criminal jus-**

tice in cyberspace – what's next? explored the ways forward to address the issues of crime and justice in cyberspace. The session focussed on several key areas including artificial intelligence, content moderation, and emerging legal frameworks[92].

The workshop examined first of all in the context of recent EU proposals to regulate the provision of online content by Internet intermediaries, the issue of online content moderation and the challenge of finding the right balance between action to remove illegal and harmful online content, and the upholding of fundamental rights including freedom of expression.

In view of the cross-border origins of much online content and the absence of universally agreed definitions of crime and terrorism, cooperation between governments and the private sector on these matters was crucial[93]. The workshop participants agreed therefore that a way forward was needed to resolve the differences between national laws, in particular concerning the definition of what was acceptable online content, while upholding the highest standards relating to freedom of expression and other fundamental rights[94].

Secondly, the workshop discussed the use of artificial intelligence (AI) technologies by law enforcement agencies. While there was general agreement that the use of AI provided new means and opportunities for tackling crime, participants from academia and business raised concerns about the potential wider effects of these tools and called for diligence in their use. It was noted in that AI applications required large amounts of resources and an advanced understanding of the technology. The resulting key EuroDIG Message provided by the workshop recommended that AI tools in law enforcement practice should not be implemented without human oversight[95], a position that had been recommended by the European Parliament[96].

The recent increase in multilateral proposals to create new norms for dealing with cybercrime was identified as yet another key issue. Concerns were raised in the workshop that proposals put forward by certain member states in the UN for a new cybercrime treaty posed the risk of duplicating efforts, increasing legal fragmentation and being likely to lead to agreements that only set minimum standards. These concerns were reflected in the workshop outcomes and the EuroDIG Messages which highlighted the importance of upholding the existing high standards established by the Budapest Convention[97].

The workshop also considered the problem raised by speakers from law enforcement and academia of the increases in the use by cybercriminals of encryption and anonymisation

which significantly obstructed criminal investigations. The session concluded with recommending alternative solutions that balanced the need for users' privacy protection while also enabling law enforcement agencies to investigate online criminal activity effectively[98].

Conclusions

12 years of important and comprehensive cybersecurity recommendations and EuroDIG Messages

Cybersecurity discussions at EuroDIG have always been based on issues identified by the EuroDIG multistakeholder community as the most relevant for the Internet governance and security agendas for Europe. Many of these issues reflect similar agendas at the UN Internet Governance Forum (IGF) and other international fora dealing with cyber issues, opportunities and challenges. The annual EuroDIG multistakeholder forum and its growing intersessional activities present to the global community of individual and business Internet users, government policymakers and law enforcement agencies, civil society experts and technical community representatives, an important regional assessment of the views, consensus positions and recommendations of stakeholders across the continent of Europe.

A key turning point in the discussions at EuroDIG occurred in 2017 when – perhaps to the surprise of many stakeholders – there was general acknowledgment that governments and regulators needed to take a leading role in the development of national and global cybersecurity policies and solutions to the emerging challenges for online security and safety. However, it was also recognised that this did not contradict the widespread support for collaborative approaches and the involvement of all stakeholders in these processes. Rather it led to calls for strengthening the multistakeholder processes with the shared aim of achieving greater trust, transparency and accountability. Governments, regulators and law enforcement agencies could not achieve these goals alone: the EuroDIG sessions on cybersecurity have consistently underlined the critical importance of engaging not only with the cybersecurity technical community and law enforcement cybercrime experts, but with all stakeholders with a direct interest in online security, safety, rights and the social and economic impacts, including governments, regulators, civil society, parliamentarians, youth representatives and academics.

To some extent this necessity for open and diverse participation reflected the complexities of the challenges associated with cybersecurity. However, underpinning this approach also has been the unstinting belief by Euro-

pean stakeholders that the opportunities and the solutions can only be developed and realised with everyone being at the table. As this chronological survey shows, EuroDIG has demonstrated in its record of success since its inception in 2008 that it provides a unique open forum for the Internet's stakeholders from the broad continent of Europe to come together with that objective firmly in mind. The outcomes of its plenary sessions, workshops and information sessions as reported in the annual EuroDIG Messages have underlined the critical importance of all stakeholder communities working together to achieve the level of sustainable cybersecurity on which the global economy now depends.

Annotations

[1] Dr. Tatiana Tropina is currently working as Assistant Professor in cybersecurity governance at the Institute of Security and Global Affairs, Leiden University. Previously she was a senior researcher at the Max Planck Institute for Foreign and International Criminal Law (2010 – 2019). This report is written based on her involvement in EuroDIG processes since 2012 in her personal capacity and does not represent the views of her employers.

[2] See: Session teaser. European perspectives on fostering security, privacy and openness on the Internet (Part II) – 2008. Available at: https://eurodigwiki.org/wiki/European_perspectives_on_fostering_security,_privacy_and_openness_on_the_Internet_(Part_II)_%E2%80%93_2008

[3] Ibid. P. 2

[4] Ibid.

[5] Cybercrime and cyber security: Public-Private Partnership – WS 04 2009. Available at: https://eurodigwiki.org/wiki/Cybercrime_and_cyber_security:_Public-Private_Partnership_%E2%80%93_WS_04_2009

[6] EuroDIG 2009. Messages from Geneva. P. 9-10. Available at: https://eurodigwiki.org/mw/images/9/97/2009_EuroDIG_Messages_from_Geneva.pdf

[7] Cross-border cybercrime jurisdiction under cloud computing – WS 01 2010. Available at: https://eurodigwiki.org/wiki/Cross-border_cybercrime_jurisdiction_under_cloud_computing_%E2%80%93_WS_01_2010

[8] See e.g. discussion paper prepared by J. Spoelne for the Economic Crime Division of the Council of Europe within the framework of the global Project on Cybercrime: Spoelne (2010), Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Available at: https://rm.coe.int/16802fa3df. The importance of standards on accessing data stored in the cloud in the context of CoE Cybercrime Convention was also highlighted by the moderator during the session introduction.

[9] Cross-border cybercrime jurisdiction under cloud computing – WS 01 2010. Session transcript. https://eurodigwiki.org/wiki/Cross-border_cybercrime_jurisdiction_under_cloud_computing_%E2%80%93_WS_01_2010

[10] Cross-border cybercrime jurisdiction under cloud computing – WS 01 2010. Session transcript. https://eurodigwiki.org/wiki/Cross-border_cybercrime_jurisdiction_under_cloud_computing_%E2%80%93_WS_01_2010

[11] Ibid. See also: EuroDIG 2010. Messages from Madrid. P. 11. Available at: https://eurodigwiki.org/mw/images/6/66/2010_EuroDIG_Messages_from_Madrid_eng.pdf

[12] Cross-border cybercrime jurisdiction under cloud computing – WS 01 2010. Session transcript. https://eurodigwiki.org/wiki/Cross-border_cybercrime_jurisdiction_under_cloud_computing_%E2%80%93_WS_01_2010

[13] EuroDIG 2010. Messages from Madrid. P. 12. Available at: https://eurodigwiki.org/mw/images/6/66/2010_EuroDIG_Messages_from_Madrid_eng.pdf

[14] EuroDIG 2011. Program overview. Available at: https://eurodigwiki.org/wiki/Programme_overview_2011

[15] Plenary 2 Cybersecurity: Cleaning-up businesses and infrastructures. Transcript. Available at: https://eurodigwiki.org/wiki/Cyber_security_%E2%80%93_cleaning-up_businesses_and_infrastructures_%E2%80%93_PL_02_2011

[16] Plenary 2 Cybersecurity: Cleaning-up businesses and infrastructures. Transcript. Available at: https://eurodigwiki.org/wiki/Cyber_security_%E2%80%93_cleaning-up_businesses_and_infrastructures_%E2%80%93_PL_02_2011

[17] Ibid.

[18] EuroDIG 2011. Messages from Belgrade. P. 12. Available at: https://eurodigwiki.org/mw/images/c/c3/2011_EuroDIG_Messages_from_Belgrade_en.pdf

[19] EuroDIG 2011. Messages from Belgrade. P. 12. Available at: https://eurodigwiki.org/mw/images/c/c3/2011_EuroDIG_Messages_from_Belgrade_en.pdf

[20] Cybercrime and social networking sites – a new threat?. Available at: https://eurodigwiki.org/wiki/Cybercrime_and_social_networking_sites_%E2%80%93_a_new_threat%3F_%E2%80%93_WS_07_2011

[21] Ibid. See also: EuroDIG 2011. Messages from Belgrade. P. 17. Available at: https://eurodigwiki.org/mw/images/c/c3/2011_EuroDIG_Messages_from_Belgrade_en.pdf

[22] Public-private cooperation in the fight against cyber-crime and safeguarding cyber security? Available at: https://eurodigwiki.org/wiki/Public-private_cooperation_in_the_fight_against_cyber-crime_and_safeguarding_cyber_security%3F_%E2%80%93_PL_05_2012

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] See: Multistakeholder approach to fighting cybercrime and safeguarding cyber security – PL 05 2013. Available at: https://eurodigwiki.org/wiki/Multistakeholder_approach_to_fighting_cybercrime_and_safeguarding_cyber_security_%E2%80%93_PL_05_2013; Security as a multistakeholder model – WS 06 2013. Available at: https://eurodigwiki.org/wiki/Security_as_a_multistakeholder_model_%E2%80%93_WS_06_2013

[27] Multistakeholder approach to fighting cybercrime and safeguarding cyber security – PL 05 2013. Available at: https://eurodigwiki.org/wiki/Multistakeholder_approach_to_fighting_cybercrime_and_safeguarding_cyber_security_%E2%80%93_PL_05_2013

[28] Ibid.

[29] Ibid.

[30] EuroDIG. Messages from Lisbon. P. 7. Available at: https://eurodigwiki.org/mw/images/b/bb/2013_EuroDIG_Messages_from_Lisbon_final.pdf

[31] Multistakeholder approach to fighting cybercrime and safeguarding cyber security – PL 05 2013. Available at: https://eurodigwiki.org/wiki/Multistakeholder_approach_to_fighting_cybercrime_and_safeguarding_cyber_security_%E2%80%93_PL_05_2013

[32] Transcript. Security as a multistakeholder model – WS 06 2013. Available at: https://eurodigwiki.org/wiki/Security_as_a_multistakeholder_model_%E2%80%93_WS_06_2013#Transcript

[33] Session report. Security as a multistakeholder model – WS 06 2013. Available at: https://eurodigwiki.org/wiki/Security_as_a_multistakeholder_model_%E2%80%93_WS_06_2013#Session_report

[34] EuroDIG. Messages from Lisbon. P. 9. Available at: https://eurodigwiki.org/mw/images/b/bb/2013_EuroDIG_Messages_from_Lisbon_final.pdf

[35] Messages. Security, Internet principles and human rights – PL 05 2014. Available at: https://eurodigwiki.org/wiki/Security,_Internet_principles_and_human_rights_%E2%80%93_PL_05_2014#Messages

[36] Ibid. See also: EuroDIG 2014. Messages from Berlin. P. 19. Available at: https://eurodigwiki.org/mw/images/3/33/2014_EuroDIG_Messages_from_Berlin_small.pdf

[37] A secure and non-fragmented cyberspace: rule of law in a cross-border environment – PL 06 2014. Available at: https://eurodigwiki.org/wiki/A_secure_and_non-fragmented_cyberspace:_rule_of_law_in_a_cross-border_environment_%E2%80%93_PL_06_2014

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] EuroDIG 2014. Messages from Berlin. P. 20. Available at: https://eurodigwiki.org/mw/images/3/33/2014_EuroDIG_Messages_from_Berlin_small.pdf

[42] Cybersecurity: bringing the puzzle together – WS 05 2015. Available at: https://eurodigwiki.org/wiki/Cybersecurity:_bringing_the_puzzle_together_%E2%80%93_WS_05_2015

[43] Ibid.

[44] Ibid.

[45] EuroDIG 2015. Messages from Sofia. P. 24. Available at: https://eurodigwiki.org/mw/images/0/05/EuroDIG_A5.pdf

[46] Cybersecurity: bringing the puzzle together – WS 05 2015. Available at: https://eurodigwiki.org/wiki/Cybersecurity:_bringing_the_puzzle_together_%E2%80%93_WS_05_2015

[47] Cybersecurity revisited, or are best practices really best? – WS 05 2016. Available at: https://eurodigwiki.org/wiki/Cybersecurity_revisited,_or_are_best_practices_really_best%3F_%E2%80%93_WS_05_2016

[48] Ibid.

[49] The future of cybersecurity in Europe – from state of play to state of art – WS 05 follow up 2016. Available at: https://eurodigwiki.org/wiki/The_future_of_cybersecurity_in_Europe_%E2%80%93_from_state_of_play_to_state_of_art_%E2%80%93_WS_05_follow_up_2016

[50] This agreement represents the summary of the discussion made by the moderator, who asked the audience whether this point captures the discussion right. The participants raised no objections to this summary. See: The future of cybersecurity in Europe – from state of play to state of art – WS 05 follow up 2016. Available at: https://eurodigwiki.org/wiki/The_future_of_cybersecurity_in_Europe_%E2%80%93_from_state_of_play_to_state_of_art_%E2%80%93_WS_05_follow_up_2016

[51] EuroDIG 2016. Messages from Brussels. P. 26. Available at: https://eurodigwiki.org/mw/images/2/25/Messages_from_Brussels.pdf

[52] Alice in wonderland – mapping the cybersecurity landscape in Europe and beyond – Pl 01 2017. Available at: https://eurodigwiki.org/wiki/Alice_in_wonderland_%E2%80%93_mapping_the_cybersecurity_landscape_in_Europe_and_beyond_%E2%80%93_Pl_01_2017

[53] Ibid.

[54] Ibid.

[55] EuroDIG 2017. Messages from Tallinn. P. 20. Available at: https://eurodigwiki.org/mw/images/c/c8/Messages_from_Tallinn_EuroDIG_2017.pdf

[56] Stress testing the multistakeholder model in cybersecurity – WS 09 2017. Available at: https://eurodigwiki.org/wiki/Stress_testing_the_multistakeholder_model_in_cybersecurity_%E2%80%93_WS_09_2017

[57] EuroDIG 2017. Messages from Tallinn. P. 35. Available at: https://eurodigwiki.org/mw/images/c/c8/Messages_from_Tallinn_EuroDIG_2017.pdf

[58] Ibid.

[59] Criminal justice on the Internet – identifying common solutions – WS 4 2017. Available at: https://eurodigwiki.org/wiki/Criminal_justice_on_the_Internet_%E2%80%93_identifying_common_solutions_%E2%80%93_WS_4_2017

[60] Ibid.

[61] EuroDIG 2017. Messages from Tallinn. P. P. 29. Available at: https://eurodigwiki.org/mw/images/c/c8/Messages_from_Tallinn_EuroDIG_2017.pdf

[62] Criminal justice on the Internet – identifying common solutions – WS 4 2017. Session transcript. Available at: https://eurodigwiki.org/wiki/Criminal_justice_on_the_Internet_%E2%80%93_identifying_common_solutions_%E2%80%93_WS_4_2017#Transcript

[63] EuroDIG 2017. Messages from Tallinn. P. 29. Available at: https://eurodigwiki.org/mw/images/c/c8/Messages_from_Tallinn_EuroDIG_2017.pdf

[64] Non-state actors in Europe and beyond: The true shapers of cybersecurity norms?! – WS 09 2018. Available at: https://eurodigwiki.org/wiki/Non-state_actors_in_Europe_and_beyond:_The_true_shapers_of_cybersecurity_norms%3F!_%E2%80%93_WS_09_2018

[65] Category: security and crime 2018. Available at: https://eurodigwiki.org/wiki/Category:Security_and_crime_2018

[66] Ibid.

[67] Ibid.

[68] EuroDIG 2018. Messages from Tbilisi. P. 28. Available at: https://eurodigwiki.org/mw/images/c/cb/Messages_from_Tbilisi_EuroDIG_2018.pdf

[69] Ibid.

[70] IoT – economic opportunities and security challenges. – WS 05 2018. Available at: https://eurodigwiki.org/wiki/IoT_%E2%80%93_economic_opportunities_and_security_challenges._%E2%80%93_WS_05_2018

[71] EuroDIG 2018. Messages from Tbilisi. P. 24. Available at: https://eurodigwiki.org/mw/images/c/cb/Messages_from_Tbilisi_EuroDIG_2018.pdf

[72] Challenges of cybercrime and transborder investigations – Flash 13 2018. Available at: https://eurodigwiki.org/wiki/Challenges_of_cybercrime_and_transborder_investigations_%E2%80%93_Flash_13_2018

[73] Category: Security and crime 2019. Available at: https://eurodigwiki.org/wiki/Category:Security_and_crime_2019

[74] Making norms work – Pursuing effective cybersecurity – PL 04 2019. Available at: https://eurodigwiki.org/wiki/Making_norms_work_%E2%80%93_Pursuing_effective_cybersecurity_%E2%80%93_PL_04_2019

[75] EuroDIG 2019. Messages from The Hague. P. 19. Available at: https://eurodigwiki.org/mw/images/9/9b/Messages_from_The_Hague_EuroDIG_2019.pdf

[76] Making norms work – Pursuing effective cybersecurity – PL 04 2019. Available at: https://eurodigwiki.org/wiki/Making_norms_work_%E2%80%93_Pursuing_effective_cybersecurity_%E2%80%93_PL_04_2019

[77] See Cybersecurity challenges ahead! How would you shape regulation to address changing technology? – WS 07 2019. Available at: https://eurodigwiki.org/wiki/Cybersecurity_challenges_ahead!_How_would_you_shape_regulation_to_address_changing_technology%3F_%E2%80%93_WS_07_2019; EuroDIG 2019. Messages from The Hague. P. 30. Available at: https://eurodigwiki.org/mw/images/9/9b/Messages_from_The_Hague_EuroDIG_2019.pdf

[78] Ibid.

[79] Ibid.

[80] EuroDIG 2019. Messages from The Hague. P. 30. Available at: https://eurodigwiki.org/mw/images/9/9b/Messages_from_The_Hague_EuroDIG_2019.pdf

[81] Criminal justice in cyberspace – more of everything? – WS 11 2019. Available at: https://eurodigwiki.org/wiki/Criminal_justice_in_cyberspace_%E2%80%93_more_of_everything%3F_%E2%80%93_WS_11_2019

[82] Ibid.

[83] EuroDIG 2019. Messages from The Hague. P. 34. Available at: https://eurodigwiki.org/mw/images/9/9b/Messages_from_The_Hague_EuroDIG_2019.pdf

[84] See: COVID-19 pandemic – lessons learned for children's safety – Pre 10 2020. Available at: https://eurodigwiki.org/wiki/COVID-19_pandemic_%E2%80%93_lessons_learned_for_children%E2%80%99s_safety_%E2%80%93_Pre_10_2020

[85] Category:Security and crime 2020. Available at: https://eurodigwiki.org/wiki/Category:Security_and_crime_2020

[86] Enhancing users' confidence in cyberspace – risks and solutions – WS 02 2020. Available at: https://eurodigwiki.org/wiki/Enhancing_users%E2%80%99_confidence_in_cyberspace_%E2%80%93_risks_and_solutions_%E2%80%93_WS_02_2020

[87] See: Enhancing users' confidence in cyberspace – risks and solutions – WS 02 2020. Available at: https://eurodigwiki.org/wiki/Enhancing_users%E2%80%99_confidence_in_cyberspace_%E2%80%93_risks_and_solutions_%E2%80%93_WS_02_2020; EuroDIG Messages 2020. Virtual Meeting. P. 24. Available at: https://eurodigwiki.org/mw/images/4/42/EuroDIG_Messages_2020-virtual_meeting.pdf

[88] Ibid.

[89] The Impact of DNS Encryption on the Internet Ecosystem and its Users – WS 03 2020. Available at: https://eurodigwiki.org/wiki/The_Impact_of_DNS_Encryption_on_the_Internet_Ecosystem_and_its_Users_%E2%80%93_WS_03_2020

[90] Ibid.

[91] EuroDIG Messages 2020. Virtual Meeting. P. 25. Available at: https://eurodigwiki.org/mw/images/4/42/EuroDIG_Messages_2020-virtual_meeting.pdf

[92] Criminal justice in cyberspace – what's next? – WS 07 2020. Available at: https://eurodigwiki.org/wiki/Criminal_justice_in_cyberspace_%E2%80%93_what%E2%80%99s_next%3F_%E2%80%93_WS_07_2020

[93] Ibid.

[94] EuroDIG Messages 2020. Virtual Meeting. P. 29. Available at: https://eurodigwiki.org/mw/images/4/42/EuroDIG_Messages_2020-virtual_meeting.pdf

[95] Ibid.

[96] Criminal justice in cyberspace – what's next? – WS 07 2020. Available at: https://eurodigwiki.org/wiki/Criminal_justice_in_cyberspace_%E2%80%93_what%E2%80%99s_next%3F_%E2%80%93_WS_07_2020

[97] Criminal justice in cyberspace – what's next? – WS 07 2020. Available at: https://eurodigwiki.org/wiki/Criminal_justice_in_cyberspace_%E2%80%93_what%E2%80%99s_next%3F_%E2%80%93_WS_07_2020; EuroDIG Messages 2020. Virtual Meeting. P. 29. Available at: https://eurodigwiki.org/mw/images/4/42/EuroDIG_Messages_2020-virtual_meeting.pdf

[98] Ibid.

About the Author

Tatiana Tropina is Assistant Professor in cybersecurity governance at the Institute of Security and Global Affairs, Leiden University. Previously, she worked as a senior researcher at the Max Planck Institute for Foreign and International Criminal Law.

In the past 10 years, she has been involved in both legal research and various applied cybercrime and cybersecurity projects at the international level, such as cybercrime study for the Global Symposium of Regulators (ITU, 2010), UNODC Comprehensive Cybercrime Study (2012 – 2013), research on the illicit financial flows and digital technologies for the World Development Report 2016, a project with German Federal Criminal Police Office on improving mutual legal assistance on interception of electronic communications in the EU (2015 – 2018), and others.

Her areas of expertise include international standards to fight cybercrime, digital investigations, self- and co-regulation to address cybersecurity issues and the multi-stakeholder approach to cybersecurity. Tatiana has a number of publications to her credit, including a monograph on cybercrime. She holds a doctoral degree from the Far Eastern Federal University (Russia) and Master's degree from the University of Strathclyde, UK.

Imprint

Published by:
EuroDIG Support Association
Schächlistrasse 19, CH-8953 Dietikon
email: office@eurodig.org
web: www.eurodig.org

Assistant Editor: Mark Carvell

This document has been prepared with the financial support of the European Commission
however it reflects the views only of the authors.

Graphic and production: monade · agentur für kommunikaton GmbH, Leipzig
2021