VOLUME 3 (2017) ▪ ISSUE 3

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

The European Cybersecurity Journal is a new specialized quarterly publication devoted to cybersecurity. It will be a platform of regular dialogue on the most strategic aspects of cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem-solving instruments.

ISSN: 2450-21113

The ECJ is a quarterly journal, published in January, April, July and October.

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows:
"European Cybersecurity Journal",
Volume 3 (2017), Issue 3, page reference

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

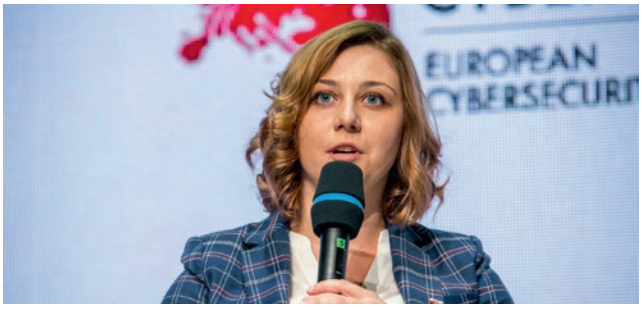
Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

www.ik.org.pl
www.cybersecforum.eu

Printed in Poland
by Drukarnia Diament | diamentdruk.pl

DTP: Marcin Oroń

EDITORIAL



DR JOANNA ŚWIĄTKOWSKA
Chief Editor of the European Cybersecurity Journal
CYBERSEC Programme Director
Senior Research Fellow of the Kosciuszko Institute, Poland

The current issue of the European Cybersecurity Journal (ECJ) is being published during the 3rd edition of the European Cybersecurity Forum – CYBERSEC. The main motto of this year's conference, 'Dealing with Cyber Disruption' reflects the key messages of the articles included in this ECJ.

Disruption is all about change – it can lead to destructive but also creative consequences. Modifications caused by digital technologies are exceptional, as they tend to significantly influence almost all aspects of our reality. Articles in the current issue of ECJ illustrate this conviction, thus providing readers with analyses of various disruptions caused by actions conducted in cyberspace.

We will have a chance to examine the constantly evolving threats landscape with a special focus on the recent ransomware attacks. We will also learn more about countermeasures that may be used to stop them. But digital technologies are not only about technical security of ICT systems. They are also about the changes that must occur within our traditional systems, including legal ones. One of the texts therefore provides us with a closer look at proposals aimed at increasing the effectiveness of the rules governing law enforcement access to digital evidence in a timely manner in order to prevent or investigate criminal and terrorist acts.

Another article focuses on one of the most burning problems that modern democracies face: cybersecurity of e-voting. This area requires increased attention from not only cybersecurity experts but also decision makers.

This issue of ECJ reveals a different nature of changes caused by the digital world, as cyberspace disturbs international relations and global peace and stability. Apart from investigating the problem, concrete initiatives aimed at reducing risk are provided in one of the articles dedicated to this issue as well as the interview conducted with H.E. Marina Kaljurand. Ensuring security in cyberspace requires strategies, relevant tools, and changes in terms of a qualified workforce. One article presented in this ECJ evaluates this need and calls for rapid and decisive action.

Finally, cyberspace has disturbed the traditional manner in which policies designed to face cyberthreats are created and implemented. Cyberspace has reshaped the status quo of main stakeholders and their power. Today, actions undertaken solely by state entities are insufficient. Multistakeholder engagement is needed and required. This approach will also be examined.

Even though a variety of approaches are covered in the current issue of ECJ, it is obvious that only a small piece of the landscape of changes has been analysed. We know very well that this is continuous process that needs to be repeated over time. We will do just that in subsequent issues of ECJ as well as through other editions of CYBERSEC.
Please join us in this journey.

CONTENTS

ANALYSIS

A MULTISTAKEHOLDER APPROACH TO CYBERSECURITY POLICY DEVELOPMENT

LEA KASPAR
Lea Kaspar is the Executive Director of Global Partners Digital (GPD). Since 2012, she has been working at the intersection of human rights and digital communications, concentrating upon facilitating multistakeholder dialogue and effective civil society engagement in international forums and processes. She is currently working on the development and implementation of GPD's cyber capacity building programme, which aims to make cyber policy-making processes around the world more open and inclusive. She is the co-Chair of the Advisory Board of the Global Forum on Cyber Expertise, a member of the Internet Governance Forum Multistakeholder Advisory Group, the UK Multistakeholder Group on Internet Governance, and the UN CSTD Working Group on Enhanced Cooperation. She is a member of the European Council on Foreign Relations.

MATTHEW SHEARS
Matthew is Lead Strategist with Global Partners Digital. In this role, he provides strategic input across GPD's portfolio of global programmes. His chief areas of focus are Internet policy and governance, cybersecurity and human rights. He has co-chaired a Freedom Online Coalition working group on human rights and cybersecurity, and has been involved in the IANA transition and enhancing ICANN's accountability over the last few years. His extensive engagement in internet governance has involved the World Summit on the Information Society (WSIS) since 2005, including the High-Level review meeting in December 2015; the World Conference on International Telecommunications (WCIT); and the Brazil NETmundial meeting. He regularly attends the Internet Governance Forum (IGF) and was a member of the first MAG.

Over the last few years, cybersecurity has evolved from a niche policy area to become a preeminent concern for governments, who have struggled to respond to the growing proliferation of cyber threats. These threats are increasingly damaging, costly, and complex. They have wide-ranging impacts across society, the economy and other policy areas. This makes cybersecurity policy development all the more challenging, and its considerations more broad and interrelated. This complexity and growing impact demand consideration of new stakeholder-driven approaches to cybersecurity policy development.

This article aims to do three things; first, review how the demand for stakeholder engagement in cybersecurity processes is growing; second, outline the characteristics of a multistakeholder process and a framework through which such a process could be implemented; and, finally, review the key elements that have to be taken into consideration when applying a multistakeholder approach to cybersecurity.

The Call For Multistakeholder Approaches To Cybersecurity Policy Development

The call for cybersecurity policies to be developed in a more open and inclusive manner does not come solely from non-governmental actors. The 2003 UNGA resolution 57/239 on the Creation of Global Culture of Cybersecurity (in particular the Annex on Elements for creating a global culture of cybersecurity) notes the importance of stakeholders working together[1]. The 2013 report of the UN Group of Governmental Experts (UNGA Report A/68/98) called on states to "encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs"[2].

The 2014 NETMundial Multistakeholder Statement[3] noted that "initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, the private sector, civil society, academia, and the technical community."

The London Process, one of the most important global forums where cyber policy is discussed, has highlighted

1 | United Nations General Assembly (UNGA), Resolution adopted by the General Assembly A/RES/57/239, on the Creation of a global culture of cybersecurity, 31 January 2003.
2 | UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98, Paragraph 24, 24 June 2013 .
3 | NETmundial Multistakeholder Statement, Section III, paragraph b, published on 24 April 2014, (online) http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf [Access 14.09.17].

the need for multistakeholder engagement and cooperative approaches to cybersecurity challenges. The Seoul Framework (outcome document of the 2013 Seoul Conference on Cyberspace) stated that it is "necessary to continue to work together towards ensuring a trusted, secure and sustainable environment in partnership with multiple stakeholders, including international organizations and the private sector[4]".

Most recently, the Chair's statement at the 2015 Global Conference on CyberSpace in The Hague urged stakeholders "to ensure that cyber policy at national, regional and international level is developed through multistakeholder approaches, including civil society, the technical community, businesses and governments across the globe"[5].

From the above, one might gain the impression that open and inclusive approaches to cyber policy-making have already taken root; have even become commonplace. In fact – with a few notable exceptions, which this paper will examine – such approaches are almost never applied to cyber policy making.

Characteristics of a Multistakeholder Approach

There has been much discussion in the Internet governance space on the merits of multistakeholder approaches to governance and policy, and the mechanisms by which they could be realized. It is important to note, however, that such approaches are not particular to the internet space. They have proven effective in other policy spheres, particularly in the environment, extractive industries, and conflict prevention and peace building[6].

4 | Seoul Framework for and Commitment to Open and Secure Cyberspace, Section 1, (online) http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf [Access 14.09.17].

5 | Global Conference on CyberSpace, 2015 Chair's Statement, Paragraph 15 (online) https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf [Access 14.09.17].

6 | See, for example, the following that stemmed from the Earth Summit in 2002 (online) http://www.wageningenportals.nl/sites/default/files/resource/multi_stakeholder_processes_for_governance_and_sustainability_hemmati_2002.pdf as well as other intiatives as outlined here: (online) www.mspguide.org/case-studies.

Before discussing how multistakeholder approaches to policy or processes can be effectively implemented, it's important to first define what we mean by such an approach. Global Partners Digital (GPD) has closely examined a range of multistakeholder approaches found in various organisations, forums and processes – both within the Internet governance field, and in other sectors (such as the environment and climate change movements). From a synthesis and consolidation of these case studies, GPD found that there are six characteristics that commonly underpin multistakeholder policy approaches. These are as follows:

1. The process is open and accessible.

All relevant stakeholders are allowed to participate in the policy process. No stakeholder is excluded on the basis of their disability, language, race, religion, gender, sexuality or culture, or as a result of high financial costs, bureaucracy or location.

2. Relevant stakeholders and their views are included.

All relevant stakeholder groups are actively represented in the policy process. Stakeholders have equal opportunities to contribute and their contributions are given due consideration.

3. The process is driven by a willingness to collaborate.

Stakeholders are willing to work together and to agree on a common purpose. This common purpose is used to determine and guide the direction of the policy process, and stakeholders remain committed to it throughout.

4. Decision-making is consensus driven.

Decision-making processes and mechanisms are based on the notion of consensus, meaning that stakeholders in the process act, as far as is possible, by general agreement.

5. Decisions are evidence-based.

Decisions are based on evidence and fact where available; the group as a whole has expertise on all of the issues relevant to the process. Where expertise

is lacking, the group has access to balanced and independent expert opinion and resources.

6. **The process and engagement are transparent and accountable.** From the outset, there is a set of clearly defined procedures and mechanisms for each different aspect of the policymaking process, covering issues such as stakeholder representation, stakeholder contributions, inclusion and exclusion of inputs, decision-making, leadership of the process, accountability, and redress.

Implementing Multistakeholder Approaches To Cybersecurity Policy

While some decision-makers are convinced by the case for multistakeholder policy development – and calls for stakeholder involvement are certainly growing – there has not been a significant increase in the number of Internet governance-related (let alone cybersecurity-related) multistakeholder policy processes. There are a number of reasons for this, including unwillingness to accept new policy development processes by governments, and the perceived or real sensitivity of the policy issue, among others.

The lack of tools and templates for setting up inclusive cyber policy processes – which, to be clear, can be complex and challenging – compounds the challenge. Without clear guidance, actors may find it difficult even to know where to begin, let alone how to assess the degree to which a policy process is inclusive or multistakeholder. In addition, multistakeholder processes cannot be implemented without significant preparation. Using the multistakeholder characteristics outlined above is, by itself, also likely to be insufficient. For such a process to work, a framework-based approach that includes agreed upon goals, timelines, decision-making processes, accountability mechanisms, and transparency is necessary.

GPD's Framework for multistakeholder policy making[7] aims to provide such a framework, offering both a means of measuring existing processes against the six characteristics listed above, and setting out and defining the four stages of policy development:

Policy process formation (including agenda-setting):
This stage establishes the protocols that will guide the policy process, including rules of engagement and mechanisms for agreeing the outputs. These protocols might take the form of a Charter, or similar document, that the parties to the process sign. The formation stage is critical to the success of the process as a whole, and should address a number of essential elements, including: mandate; goals; participation; existing policy or legal considerations; timeline; resources available (financial and otherwise); data and evidence; facilitation/leadership; and work processes including (importantly) decision-making.

Policy drafting:
The number of steps within this stage will depend both on the issue and on national policymaking norms or frameworks and could include: research and mapping; consultation (public and expert); drafting; and review. The policy drafting process is not a linear process, and some or all stages may be repeated several times.

Policy agreement:
This is the stage of the process in which the parties in the policymaking process come to agreement – typically through consensus – on the policy in question. If agreed, the policy is then forwarded on to those parties who are in a position to adopt the policy (stage 4). If the policy is not agreed upon, then it would, subject to protocols agreed in stage 1, be further worked on by the stakeholders.

Policy adoption:
This is the final stage in the process, during which policy is adopted. The extent to which the mechanism for the adoption of the policy is multistakeholder will largely depend on both the nature of the policy and the requirements for adoption. For example, in the case of voluntary agreements, adoption may well be just a matter of agreement among those parties engaged in the policy development process. If the policy requires legislative implementation, then adoption would rest with a governmental body.

7 | See more on the Global Partners Digital's website: www.gp-digital.org/publication/framework-for-inclusive-cyber-policymaking.

This framework approach seeks to be both comprehensive and yet flexible enough for any stakeholder to use – be it government, civil society, business, the technical community, academia, or a user. How and why each stakeholder might use the tool will vary depending on their priorities. For example, civil society may use a framework to identify important gaps in the cyber policy process so that they can better focus their advocacy efforts. They may also use it to demonstrate how meaningful an existing national 'multistakeholder' process actually is, so that it can be improved. Governments may, in turn, use it as a tool for mapping and implementing policy processes, setting up a new multistakeholder process, for self-reflection, or to showcase themselves as models for best practice.

Cybersecurity Specific Considerations When Implementing a Multistakeholder Approach To Policy Processes

Multistakeholder processes can appear cumbersome, time-consuming and difficult to implement. These challenges – which exist in any policy area – are particularly acute in cybersecurity, where few precedents exist for multistakeholder policymaking, and national security concerns can often exert a preponderant influence. Yet through adopting a clear understanding of what the characteristics of multistakeholder approaches are, and by implementing a well-structured process using a framework approach, a number of the real or perceived impediments to implementing such processes can be eliminated.

Of course, there is no one 'right way' to do multistakeholder policymaking. Approaches will always vary depending on a range of factors, including: the nature of the specific policy issue; stage in the policy process; the local context; the policy processes and institutional structures already in place; and the capacity and skills base of the actors involved. But a framework approach as outlined above may provide a useful starting point to facilitate the development of multistakeholder cyber policy processes.

There are additional considerations when implementing a multistakeholder process in the cybersecurity space. For example, the scope and impact – across society and economy – of the cyber issue may be significantly wider than for other Internet policy issues. The issue may be more complex given the security implications, involving a broader range of specialized expertise. The existing policy and legal considerations may also be broader and have international implications. The considerations for human rights and the rule of law may be more pressing, particularly if there is a national security dimension to the policy issue. The latter may introduce additional access restrictions; for example, documents or discussions may be available only to those with a specific security clearance.

None of these challenges are insurmountable, or diminish the critical importance and demand for greater stakeholder engagement in cybersecurity policymaking. In fact, it could be argued that the scope of these considerations makes this demand even more urgent and pressing.

Conclusion: The Pressing Need For New Policy Approaches To Cybersecurity

Calls from governments and non-governmental actors for multistakeholder approaches to cybersecurity policy development are growing. This is largely in recognition of the increasing complexity, cross-border nature, and society-wide impact of cybersecurity challenges and threats. Putting in place multistakeholder processes is neither easy, nor, without the proper approach and structuring, is it guaranteed success. However, as outlined above, a framework-based approach to multistakeholder cyber policy development provides the structure and appropriate set of guiding characteristics that will increase the likelihood of success. Without such an approach, multistakeholder approaches are unlikely to result in the actual benefits such processes are capable of.

The challenges posed by cybersecurity across all areas of human life are of such magnitude and complexity that current policy responses – largely closed, and led solely by governments – are unlikely to be sufficient, and may result in increased collateral damage and further

vulnerabilities. Bringing in the voices of other stakeholders, with their breadth of expertise and perspectives, makes targeted and effective responses more likely. Such a paradigm shift would deliver great benefits and increased security to society and economy in general.

The authors gratefully acknowledge the constructive input on structure and content of the article by colleagues Jonathan Jacobs and Daniela Schnidrig. ■

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship project in the field of cybersecurity, within which the CYBERSEC Forum is organized.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY JOURNAL