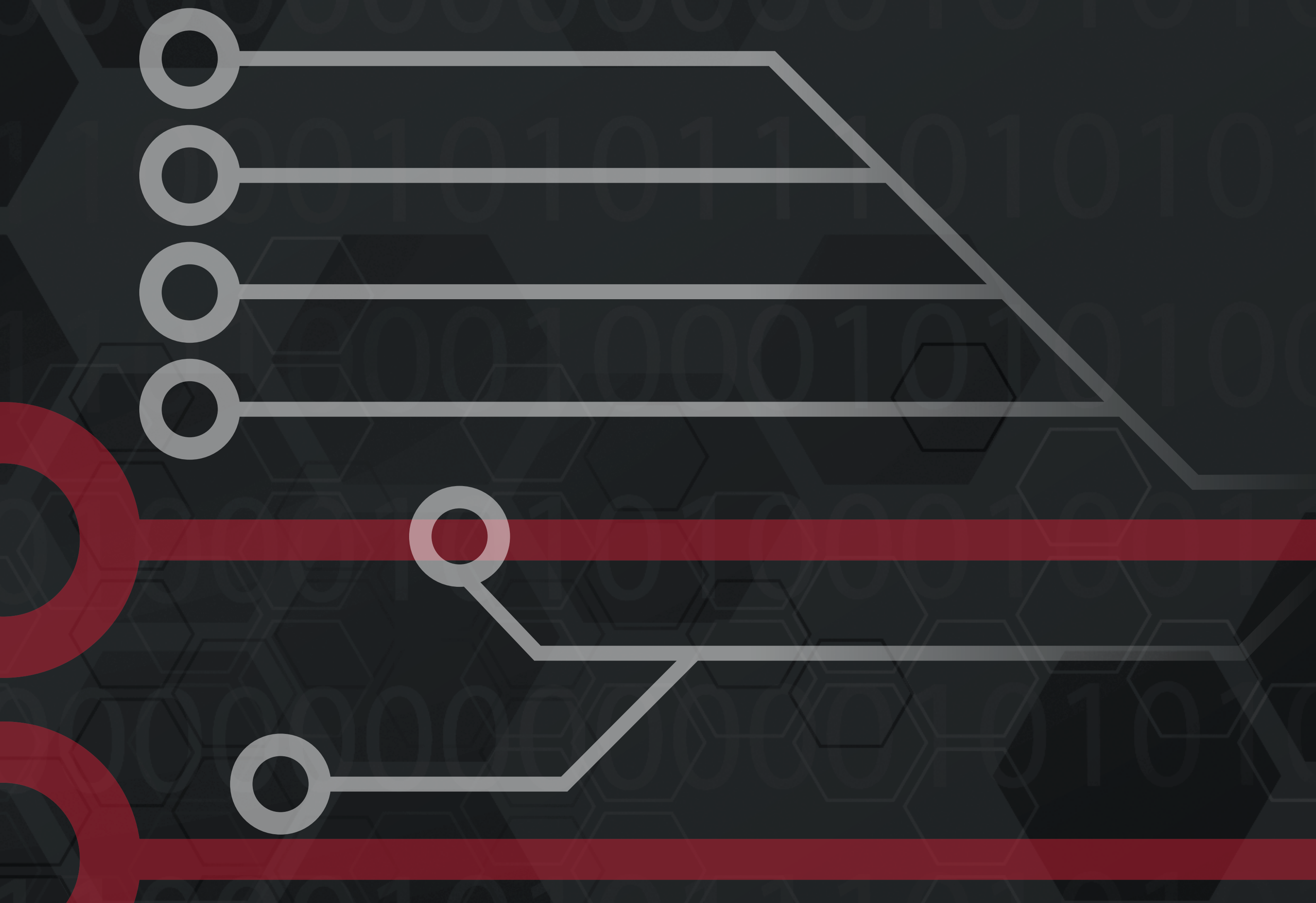
VOLUME 3 (2017) ▪ ISSUE 3

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.

EDITORIAL BOARD

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

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

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.

Joanna Świątkowska

CONTENTS

INTERVIEW WITH H. E. MARINA KALJURAND

AMBASSADOR MARINA KALJURAND
Marina Kaljurand is the Chair of the Global Commission on the Stability of Cyberspace and a Former Minister of Foreign Affairs of Estonia (July 2015-October 2016). She began her career at the Ministry of Foreign Affairs in 1991 and had since held several leadership positions, including Undersecretary for Legal and Consular Affairs (Legal Adviser), Undersecretary for Trade and Development Cooperation, Undersecretary for Political Affairs. She has also been appointed as Ambassador of Estonia to several countries. She has played an important role as expert and negotiator in the process of Russian troop withdrawal and in negotiations on land and maritime boundaries agreements between Estonia and the Russian Federation, as well as in the accession negotiations of Estonia to the European Union and to the OECD.

Marina Kaljurand has been appointed twice to serve as the Estonian National Expert at the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, in 2014-2015 and currently. Marina Kaljurand graduated cum laude from Tartu University (M.A. in Law), she also has a professional diploma from the Estonian School of Diplomacy and a M.A. degree in International Law and Diplomacy from the Fletcher School of Law and Diplomacy, Tufts University. She has been awarded the Order of White Star, III class, and the Order of the National Coat of Arms, III class, by the President of Estonia.

Your Excellency, the first full meeting of the Global Commission on the Stability of Cyberspace, held in Tallinn on 2–3 June 2017 constituted a critical step in establishing a future blueprint for the Commission's engagement. What are the main goals and priorities for the work program for the upcoming three-year mandate?

The Global Commission on the Stability of Cyberspace (GCSC) was launched in March 2017, at the Munich Security Conference. The GCSC comprises 27 independent Commissioners representing a wide range of geographic regions, from Berkeley to Beijing, as well as government, industry, academia, technical and civil society stakeholders with a very wide range of expertise. The work of the Commission is supported by the Research Advisory Group.

The objective of the Commission is to develop proposals for norms and policies to enhance international security and stability, and to guide responsible state and non-state behaviour in cyberspace. The GCSC engages a full range of stakeholders to develop shared understanding and advance cyber stability by supporting information exchange, capacity building, basic research, and advocacy.

The first full GCSC meeting in Tallinn on 2-3 June 2017 discussed the working program and prioritized topics for 2017–2018, including „the public core of the Internet" and „critical infrastructures", and the protection thereof. As a first step, the GCSC focused on a working definition of critical infrastructure: the public core of the Internet, critical infrastructures of the Internet, and IT aspects of non-Internet critical infrastructures.

The GCSC also touched upon other topics, such as the protection of electoral infrastructures, the application of sovereignty, secure access for the next billion users, rules for offensive actions in cyberspace, attribution, compliance to norms, and private sector responsibilities.

The GCSC will be transparent about its work and will inform about its deliberations. As the Chair of the GCSC I hope that the GCSC will find its unique role in the international arena by cooperating with other international organisations and platforms, and engaging with many different experts from a very wide geographical arena[1].

How could you explain the idea behind the notion of stability of cyberspace? In other words, why do we need initiatives like the Commission?

There are different definitions of stability (security) of cyberspace. For example, the UN GGE refers in its reports to „open, secure, stable, accessible and peaceful ICT (cyber) environment". All these elements are important corner stones and relevant parts of cyber stability. Today, there are many international organisations/forums that discuss cyber stability/security. I would argue that international community has accepted that there cannot be stable and secure global cyberspace without international cooperation and predictability defined by adherence to international law and agreed political/non-binding norms of responsible state behaviour. Therefore, international discussions leading to better understanding and common positions are of utmost importance. I would also argue that all international organisations and platforms dealing with cybersecurity have their place, role, and objective. Some of them are more successful than others; some of them are global, and others are regional; some of them include only states/governments, while others have a wider range of participants. But I do not know today any other relevant organisation or platform addressing cyber stability that is global in its nature and includes very different stakeholders, from professors to technical experts, from former ministers and security advisers to representatives of industry, from former hackers to human rights activists. Extraordinary personalities, exceptional experience, and wide geographical representation make the GCSC unique and perfectly suited to consolidate global efforts for cyber stability/security.

Establishing rules for offensive actions in cyberspace seems particularly important in the complex system of issues critical to the stability of cyberspace. How does the Commission plan to tackle this problem?

As you can see from my answer to the first question, the "rules for offensive actions" are among the topics that the GCSC will address. I do not want to speculate about future discussions, but I will be happy to share in due course the focus and results of the discussion in the GCSC.

How do you see the role and responsibilities of the private sector in making cyberspace a more secure domain?

The private sector has a very important role in cybersecurity for several reasons. First, the private sector owns a very significant part of critical infrastructure; second, it provides the majority of e-services; and third – the private sector, with its unique experience and highly qualified experts, is an indispensable partner to governments and other stakeholders in cybersecurity. Estonia has an unparalleled experience of cooperation with industry as well as of public-private partnerships in cybersecurity. It goes back to 2007, when Estonia was the first country in the world to fall under politically motivated and well-coordinated cyberattacks against a sovereign nation. Those DDOS attacks were neither destructive nor did they hurt anybody, but they were disturbing for a country that had adopted and enjoyed e-lifestyle for some time already and taught us useful lessons. Experts from the private sector, including banking, were the first ones to come to assist the government in tackling those cyberattacks. The Cyber Defence League, a cyber unit of the national voluntary military organisation, was formed in 2008 and since then the Unit has been an irreplaceable partner to the government. One of the lessons we learned in 2007 was the understanding that cybersecurity needs an "all-nation approach" – a real partnership between the government, the private sector, academia, technical experts, and the civil society.

[1] | For more information please visit the website: https://cyberstability.org.

The same could be said about the international level. I agree with those who say that governments have a leading role in cybersecurity, including interpreting international law, adopting norms of responsible state behaviour, awareness-raising efforts etc., but governments also have the obligation to cooperate with other stakeholders, particularly the private sector. Governments have to talk to the private sector, to listen to it, to learn it, and to cooperate with it. We have globally some outstanding examples of industry's engagement and very responsible behaviour in cybersecurity. I would like to bring one example – Microsoft. Microsoft has to be recognized for its commitment to propose norms for states and industry, to address attribution, IoT etc. We might not agree with all ideas and proposals, but Microsoft has to be acknowledged for being active and committed, for encouraging states/governments as well as other stakeholders to not only listen to what the private sector has to say, but start serious and open dialogues. At the end of the day, we all have the same objective – safe and secure cyberspace. I am very proud that Microsoft plays an important role in the work of the GCSC. I would like to assure that for the GCSC, industry/the private sector is a very valuable partner and I would like to encourage the private sector to follow the Commission's work and get in touch with the GCSC.

Recently, there have been reports of serious turbulences affecting the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. How do you interpret this information? Do you feel that the international community has reached the limit of possible cooperation in terms of building and implementing norms of responsible behaviour?

I had the honour to participate in the GGEs of 2014–2015 and 2016–2017. For me personally, it was a valuable experience and an opportunity to contribute to global efforts to make cyberspace safe, stable and secure. I am convinced that the UN as a global organization is well placed to lead global discussion and formulate policies, guidelines, and recommendations towards secure and stable cyberspace. Previous GGEs had been useful tools/mechanisms to that end, with one exception. Therefore, it is extremely disappointing that the 2016-2017 GGE failed – that the Group could not agree a consensus report.

Pursuant to General Assembly resolution 70/237, the GGE was mandated by the Secretary General "to continue studying, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, and how international law applies to the use of ICTs by States, as well as norms, rules and principles of responsible behaviour of States, confidence building measures and capacity building..."

The Group had some good discussions and made progress in all sections mentioned in the mandate, with only one exception –the applicability of international law. It was very unfortunate and regrettable that some experts did not want to have a substantial discussion on the applicability of international law. On the contrary – they kept repeating political statements and were not even ready to reconfirm what was agreed in 2013 and 2015 Reports – the fact "that international law, in particular the Charter of the United Nations in its entirety, is applicable and essential to maintaining peace and promoting an open, secure, stable, peaceful and accessible ICT environment."

The failure of the GGE is also very disappointing to the international community and the experts and states who did not participate in the work of the GGE, but who were following the discussion very carefully and expected a consensus report building on the previous reports.

So, what next? After this failure, it is difficult to imagine a new GGE in the near future. The fiasco of the 2016–2017 GGE made it very clear that this format is not working, and it does not look like it will be, at least not in the near future. At the same time, though, I think that we need some kind of a dialogue in the UN framework. We just have to be very realistic –the new format, whatever it will be, will most probably bring no substantial progress or result and is most likely to be a mere political and awareness-raising effort. Also, there is a growing need for a number of countries to continue the discussion, not only for the sake of it, but to reach some concrete agreements, inter alia, on some aspects of the applicability of international law and norms of responsible state behaviour. In Estonia, we have a saying that "nature does not like an empty spot". I am sure that the gap left by the GGE will be filled by other forums. I also strongly believe that the GCSC has its role to play. At a small GCSC Commission meeting in Las Vegas a couple of weeks ago we discussed the situation after the failed GGE and agreed to continue with some questions that had also been addressed by the GGE, e.g. the protection of critical infrastructure. The GCSC will not replace the GGE or any other existing format/platform, but the GCSC can contribute to the present and future discussions about cyber stability and security. ■

Questions by:
Dr Joanna Świątkowska

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].

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

[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.

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. ■

ANALYSIS

GROWING THE NEXT GENERATION OF CYBER PROFESSIONALS

BROOKE GRIFFITH
is the Vice President, International Business Development for Raytheon Intelligence, Information & Services (IIS) leading international business growth initiatives for one of Raytheon's four major businesses. He has responsibility for ensuring that all Raytheon global resources are integrated to help grow IIS internationally, and is the IIS representative on the Raytheon International Council. Griffith joined Raytheon in 2003 from Elemica, Inc., the primary Internet consortium for the global chemical industry, where he was Director of Business Development. Griffith earned a Bachelor's Degree in Political Science from Miami University (Ohio) and a Master's in National Security Studies from Georgetown University. He is also a graduate of the Advanced Executive Program at UCLA's Anderson School.

Cybersecurity threats today are growing at a rapid rate – even faster than internet usage itself[1]. At the same time many commercial and defence technologies are increasingly reliant on networked capability. Cyber technology innovation is ramping up to support these growing needs, but the critical challenge worldwide remains the need to develop a capable cyber workforce to maintain both national security and economic interests. With major breaches and attacks trending in headlines almost daily, government leaders and educators must address the talent gap and generate more interest in cybersecurity careers. The private sector, government, and educational institutions need to work together to help inspire our next generation of innovators and cyber defenders.

1. The Current Cyber Landscape

As a global company, Raytheon has witnessed and engaged in a variety of approaches to how countries are reassessing their cybersecurity strategies across both the public and private sectors to manage the growing cyber threat more effectively.

In the U.S., cybersecurity initiatives have focused on protecting defence assets, providing homeland security, including the protection of critical systems and infrastructure, and private-sector innovation, allocating $19 billion to cybersecurity in 2017 by some estimates[2]. To drive these initiatives forward, the U.S. government has supported cyber threat information sharing as a critical

[1] | Nelson S., NPR, 2017 [Online] www.npr.org/2017/06/29/534835108/how-europe-is-grappling-with-increased-threats-to-cybersecurity (access: 18.08.2017).

[2] | Ibidem.

policy mechanism and also dedicates significant financial resources to cyber training programs.

> “ With major breaches and attacks trending in headlines almost daily, government leaders and educators must address the talent gap and generate more interest in cybersecurity careers.

In the EU, spending estimates are lower, though rapidly increasing[3]. Significant emphasis is placed on protection of citizen data and NATO/EU cooperation versus critical infrastructure. Recent approval of the EU General Data Protection Regulation, for example, ensures that cyber-breach notification will become mandatory in all member states (within 72 hours) where an incident is likely to result in a risk for the rights and freedoms of individuals[4]. The EU approach has been effective to date against attacks carried out at the micro-level, targeting individual citizens and businesses. However, macro-level attacks, with a view to destabilising government organisations and national economies, are more prevalent than ever before. State and non-state organisations are replacing criminal actors as the primary, and more sophisticated, threat. In tandem, there has been a sharp increase in attacks against critical infrastructure[5]. The time lag between cyber intrusions and detection has hindered efforts to counter these often debilitating attacks[6]. The EU and European countries have embraced enhanced cyber policy in an effort to reduce the threat. Similar to the rest of the world, these nations will remain under a significant threat until they address an underlying problem – a shortage of cyber professionals trained to counter these complex cyberattacks.

2. A Widening Gap: Knowledge vs. Application

While many students pursue advanced degrees in cybersecurity-related fields, the human skills shortage remains the weakest link for cyber defence. European countries have fundamentals upon which to build a strong cyber talent base. Poland, for example, has more STEM (science, technology, engineering, and mathematics) graduates than most countries in Europe, but has one of the greatest shortages of IT (information technology) workers – around 40,000 people[7]. Bridging that cyber-talent gap relies on addressing the divide between academic knowledge and practical application. By 2022, Europe’s overall cyber-talent shortage is projected to reach 350,000 workers according to a recent report[8].

> “ While many students pursue advanced degrees in cybersecurity-related fields, the human skills shortage remains the weakest link for cyber defence.

Traditional educational institutions – whether providing courses specifically about cybersecurity or related fields – only meet part of the need when it comes to addressing the skills gap and training a capable cyber workforce.

[3] Ibidem.

[4] Burgess, M., GDPR will change data protection – here's what you need to know, “WIRED UK” 2017 [Online] www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (access: 24.08.2017).

[5] Seals, T., 40% of ICS, Critical Infrastructure Targeted by Cyberattacks, “Infosecurity” 2017 [Online] www.infosecurity-magazine.com/news/40-of-ics-critical-infrastructure/ (access: 24.08.2017).

[6] European Political Strategy Centre, Building an Effective European Cyber Shield, “Strategic Notes” 2017 [Online] https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en (access: 24.08.2017).

[7] Albrycht I., Education as a key factor in the process of building cybersecurity, “European Cybersecurity Journal” 2016, Vol 2 Iss 1, p. 43-47.

[8] Ashford W., ComputerWeekly, 2017 [Online] www.computerweekly.com/news/450420193/Europe-faces-shortage-of-350000-cyber-security-professionals-by-2022 (access: 18.08.2017).

University-level computer science courses have tended to take an academic approach to cybersecurity issues. While strong on theory, IT, and computing fundamentals, these traditional information security courses have typically not provided much hands-on training and skills application – and both are needed for effective cybersecurity. In a rapidly changing, dynamic measure-counter-measure environment of cyber threats, cyber professionals need to be trained in rapid analysis and response, and the curriculum must adapt quickly to keep up.

> “ Traditional educational institutions – whether providing courses specifically about cybersecurity or related fields – only meet part of the need when it comes to addressing the skills gap and training a capable cyber workforce.

This is difficult for universities. Similar to a first responder or soldier, this training only comes through repeated exercises across several scenarios in a simulated, though realistic, environment.

Professional certifications in cybersecurity serve as effective complements to the strong academic fundamentals mentioned above. For example, the Certified Information Systems Security Professional (CISSP) certification is a well-known cybersecurity qualification that is globally recognised and sought after in key cybersecurity positions. CISSPs are held to standards related to both the technical and operational skills, as well as the managerial competencies required to protect organisations from cyberattacks. Candidates must prove their mastery of engineering as well as operational security issues. Firms like Cisco Systems also offer their own certifications targeted at skill levels ranging from Entry to Expert. One such is the Cisco Certified Network Associate (CCNA) Cyber Ops certification, which prepares candidates to begin a career working with cybersecurity analysts within security operations centres. These standards are common, consistent, and transferrable across public and defence domains alike. The path toward earning certifications like these therefore serves as tangible training for the job.

When combined with traditional disciplines found in universities (e.g., engineering, mathematics) and the experience that expert-level cyber analysts and reverse engineers can provide, certification programs can help round out the wide-ranging skills that are needed for the cybersecurity mission. There is no silver bullet in terms of cyber-workforce planning; instead, a mix of capabilities is required. Cyber academies are emerging as effective fora in which to combine academic and practical training in context, from entry level technicians, to managers, to senior level practitioners.

3. Training through Partnership

To meet the immediate hiring needs in Europe and combat rising cyberthreats, EU governments must encourage partnerships between academic institutions and the private sector. Cybersecurity roles require creative thinking, curiosity and problem-solving skills that can come out of a multidisciplinary approach. Only one-fifth of the current cyber workforce in Europe comes from non-computing-related backgrounds, with 63 percent at manager level or above[9]. Recruiting the students with the right characteristics and mindset for cybersecurity professions is a prevalent challenge everywhere.

> “ There is no silver bullet in terms of cyber-workforce planning; instead, a mix of capabilities is required.

[9] | Wilson R., Recruitment International, 2017 [Online] www.recruitment-international.co.uk/blog/2017/06/europe-demanding-worlds-fastest-cybersecurity-workforce-growth-survey-finds (access: 18.08.2017).

Governments, academia, and the private sector must think proactively, then, about how best to leverage the diverse talents of their entire workforce to meet the cyber challenge. Opportunities in cyber should be thought of in a broader context than simply careers in cyber operations. Law students, for example, might be encouraged to explore minors in cybersecurity to address risk factors in the legal domain. Healthcare administrators might be encouraged to study cyber in order to better meet the unfolding challenges in data protection and threats to industrial devices and control systems in their fields. EU governments must work with their academic institutions and companies to think about the future cyberthreat in a comprehensive manner. The private sector must, in turn, clearly communicate to academia and their governments what skills and traits they are seeking in job candidates within critical sectors, and how their requirements are evolving.

Without any exposure to the cybersecurity function and career track early on, young adults may discount the growing opportunities and pursue other fields. A recent survey commissioned by Raytheon showed that during high school or secondary school, 64 percent of young adults ages 18-26 in Europe said no teacher or counsellor ever mentioned the idea of a career in cybersecurity[10]. Further compounding this problem is the lack of real-life mentors. Two-thirds of young adults (66 percent) said they had never met or spoken to a practicing cybersecurity professional[11]. These results were in line with other parts of the world.

Education, professional mentoring, extracurricular programs, and hands-on training are required to reverse this trend and begin building a strong pipeline of cybersecurity professionals. Governments can engage by promoting awareness around the cyberthreat, as well as the opportunities associated with it. One path might be to support formal (or informal) rotational programs between their agencies and industries in order to provide exposure across the many aspects of cyber. Each skill builds on, and enhances, the others.

> “ Education, professional mentoring, extracurricular programs, and hands-on training are required to reverse this trend and begin building a strong pipeline of cybersecurity professionals.

Active collaboration between business sectors, the government, and both higher and lower education systems will help foster more cyber talent. This multifaceted approach will enable future generations to become the sharp, aware, and talented cyber defenders Europe needs.

4. Closing the Gap

Cyber has become a new dimension of conflict, and organisations and countries across the world are developing their own cyberdefences in unique ways. In an effort to balance the currently inadequate supply of cyber professionals with the specialised demands of our changing environment, the following best practices should be considered by policy makers as they work with government bodies and the private sector alike to bolster their cyber workforces:

1) Seek to design training for the job
2) Strive for common criteria, targeted at objective best practices
3) Keep training coursework current
4) Encourage mentorship and partnerships
5. Implications

As mentioned earlier, there are many different roles that contribute to an organisation's cybersecurity, from entry-level positions to seasoned expert analysts. Training tracks should be linked to discrete work positions.

[10] Raytheon, Securing Our Future: Closing the Cybersecurity Talent Gap, 2017 [Online] www.raytheoncyber.com/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf (access: 18.08.2017).
[11] Ibidem.

> “The inclusion of certification programs within comprehensive training architectures will ensure consistency in an otherwise unpredictable arena.

For example, a CSOC (Cyber Security Operations Centre) operator would require a unique set of courses as compared to a digital threat hunter. Consider as well that certain knowledge and skills can only be obtained through repeated, realistic hands on cyber exercises, so training modules should emphasise applying knowledge through hands-on lab time in realistic virtual environments. Course completion should require the successful completion of practicals.

Training courses should be based on a standardised process that leverage best practices. The inclusion of certification programs within comprehensive training architectures will ensure consistency in an otherwise unpredictable arena. Consider pursuing well-known industry certifications that ensure high standards are met and that provide for the transportability of cyber professionals between organisations.

Training courses must also have automated update processes, online refreshers and technology updates to ensure professionals maintain currency and fluency. This approach must be applied to all levels of an organisation, from those who access the network infrequently to senior cyber analysts. The threat will continue to evolve at a rapid pace, and the modules must maintain their relevancy.

Awareness around cyber opportunities must improve globally and in Europe. When asked whether they were aware of the typical responsibilities and job tasks involved in a cyber profession, 53 percent of young adults in Germany said “no”[12]. Across Europe, nearly one-third (31 percent) of young adults believe they are not qualified for cyber careers[13]. Governments, academia and the private sector can play an important role in driving greater awareness to address the skills shortage. Again, engage all levels of the organisations when deploying training, going beyond IT resources to include all departments and functions. A broad approach will ultimately result in increased awareness and improved resiliency of operations. Further, consider supporting cyber competitions to improve the technical skills of each stakeholder, and strengthen each nation’s cyber community at the same time.

Dedicated cyber academies have proven to be very successful in implementing these best practices and developing skilled cyber professionals in countries around the world. They can be leveraged to prepare and certify cyber professionals to perform at the advanced levels our organisations demand.

> “Training courses must also have automated update processes, online refreshers and technology updates to ensure professionals maintain currency and fluency.

Cyber academies can also be utilised to complement the academic training offered by universities, as well as generic private sector offerings that we’ve seen in the market place. Through offering certification courses, academies provide consistent, transferrable, and practical training. Most importantly, cyber academies can be leveraged to directly satisfy vacant cybersecurity positions that organisations have now, and that they are planning for in the future. They can be another tool to grow the next generation of cyber professionals. ■

[12] Op. cit. Raytheon.

[13] Ibidem.

INTERVIEW WITH LIIS VIHUL

LIIS VIHUL
is Chief Executive Officer of Cyber Law International, a company that provides capacity building trainings and consultancy services in international cyber law. She also serves as co-editor of the International Humanitarian Law Group in the Manual on International Law Applicable to Military Uses of Outer Space project and Deputy Chair of the newly founded Global Commission on the Stability of Cyberspace's Research Advisory Group. Previously, she spent 9 years as a senior analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence, where she was the managing editor of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. She holds master's degrees in law from the University of Tartu and in information security from the University of London.

Could you please share with our readers some of your experiences related to the drafting of the Tallinn Manual 2.0? In particular, how satisfied are you with the results? Were all the assumed goals achieved? What were the greatest challenges in the drafting process? Which areas were the easiest to achieve consensus and which topics caused the most heated discussions?

After the completion of the first edition of the Manual, which looked at how international law regulates cyber warfare, our goal in the Tallinn Manual 2.0 was to understand how the law applies to cyber operations that occur in peacetime. We quickly realized that in order to do so, we needed to consider a wide array of legal regimes and principles – the issues ranged from sovereignty and jurisdiction to diplomatic and space law. The multitude and variety of topics made drafting the Tallinn Manual 2.0 extremely challenging. Although users of the book will ultimately determine how satisfactory it is, I believe we achieved a good result. On certain matters, such as sovereignty or the law of the sea, the book provides comprehensive guidance, whereas on others, for instance human rights law, it maps the key issues, thereby providing the individual who has to assess a cyber operation a jump start in his or her analysis.

Coming to a consensus wasn't a major problem because we were committed to setting forth all reasonable interpretations of the law. Indeed, the book is filled with examples of situations in which the experts interpreted the law differently. This is probably the greatest value of the book; it alerts the reader to those questions of law where there is no single answer. Instead, our primary challenge arose earlier in the process, as we were writing the first drafts of the chapters. Because most of the legal regimes had never been analysed in the cyber context before, we were starting from scratch. As a result, some of the chapters required quite a few rewrites until we were convinced that we had set out the law, and the varying interpretations of that law, fully and fairly.

There have been numerous attempts to create instruments governing the use of cyberspace. Examples include the Council of Europe Convention on Cybercrime, the EU Network and Information Security (NIS) Directive, the United Nations Group of Governmental Experts 2015 Report, and the 2015 US-China bilateral Declaration. Could you please identify the areas which in your opinion are the most urgent to be regulated under international law?

To be honest, I don't think there is any particular issue that demands immediate legal regulation. This is not to say that such issues do not exist, but simply that subjecting any cyber matter to international legal regulation would be premature at this point in time. Let's take the proposition that the scope and scale of cyber espionage activities somehow needs to be curbed. It is easy to say that a treaty to that effect is needed. The reality is, of course, much more difficult than that. Treaty negotiation would be an extremely long undertaking and unlikely to attract global support. And even if a treaty restricting cyber espionage were negotiated, what would its verification and enforcement regime look like?

I therefore believe that to the extent issues can be solved by interpreting existing law instead of attempting to create new law, interpretation should be the preference of states.

When it comes to the applicability of International Humanitarian Law (IHL) or Law of Armed Conflict (LOAC) to cyber operations, do you believe there is a requirement for changes or adaptation? Or are the existing LOAC instruments sufficient to address cyber operations and it would be enough to apply them mutatis mutandis, having in mind, among others the Martens Clause?

IHL is one of the more developed fields of international law and undoubtedly the most researched legal regime with respect to cyberspace. That research tells us that cyber operations that occur during armed conflict, such as those carried out in the Syrian civil war, raise unique issues of IHL. Does the law therefore need to be changed? I don't take this view. Rather, I believe that again, interpretation is the answer. IHL is sufficiently dynamic to accommodate the cyber challenge.

The U.S. is considering declaring the whole electromagnetic spectrum (supposedly including cyberspace) as a domain of warfare. What challenges – from the perspective of International Law – do you think the U.S. will face in this regard?

Treating cyberspace as a domain of warfare raises no legal challenges per se because the law does not treat cyberspace as a war-free domain. To the extent war is fought in cyberspace, it must comply with the applicable international law rules.

In your opinion what are the main differences in the approach to cyber operations between the U.S. and European NATO Members?

With respect to their views on the law, there aren't many differences. In fact, countries on both sides of the Atlantic have not been very specific about how they apply and interpret international law in the cyber context. One might believe that the United States, due to its superior capabilities, would prefer less legal clarity and more permissive interpretations of the law, both of which would enable it to operate more freely on cyberspace. In reality, the United States has been quite forthcoming on how the law should be applied vis-à-vis cyberspace. Many European states, however, are in the early phases of cyber capability development. For them, it might therefore be premature to articulate very specific interpretations of the law.

Lastly, please point to cybersecurity-related areas in which you believe broadly understood international cooperation requires tightening or improvement.

The difficult situation of international security also determines, at least to an extent, the status quo of international cyber security. With this summer's failure of the UN-led process to agree on articulations of how international law applies in cyberspace, states are left with the dilemma of how to continue their discussions. At least for the immediate future, I am more optimistic about the success of a bottom-up approach to cooperation, including on international law matters – joint exercises, unofficial information exchanges, international capacity building training, and the like. On the formal state-to-state level, cooperation will inevitably need to become more focused and less abstract – what are the specific problems that states are trying to solve, what are the optimal solutions thereto, which compromises are states willing to make, and which issues will definitely be left off the negotiating table? ■

Questions by:
Cdr Wiesław Goździewicz

ANALYSIS

DIGITAL SECURITY & DUE PROCESS: MODERNIZING CROSS-BORDER GOVERNMENT ACCESS STANDARDS FOR THE CLOUD ERA

KENT WALKER
Kent is the Senior Vice President at Google, responsible for Legal, Policy, Trust & Safety, and Google.Org. He advises Google's board and management on legal and policy issues. He oversees Google's legal and compliance affairs, its work with governments around the world, its policies for content on its various services, and its philanthropic efforts. Before joining Google, Kent held executive positions at leading technology companies. He served as an Assistant U.S. Attorney with the U.S. Department of Justice and advised the Attorney General on technology policy issues. Kent graduated with honors from Harvard College and Stanford Law School. He currently serves on the Harvard Board of Overseers and the Mercy Corps Social Ventures Fund, and is a member of the Council on Foreign Relations.

Democratic countries around the world strive to keep their citizens safe. Those governments need access to digital evidence, which can often be held by foreign communication service providers. Today's international legal frameworks, however, were built for a gone-by era when the need for cross-border evidence collection was rare. As a result, countries struggle to find ways to get the information they need, and the solutions proposed often come at a high cost for privacy and security. The proposals in this document would allow law enforcement authorities to obtain the digital evidence they need to investigate legitimate cases in a more timely manner while protecting privacy.

The Problem...	The Solution...
Governments that adhere to baseline privacy, due process, and human rights standards are encumbered in their ability to obtain electronic data that is held by service providers. These governments have legitimate law enforcement objectives, and they are often unable to obtain this data in a timely manner...	... Digital evidence that is held by service providers should be accessible in a timely manner for legitimate law enforcement investigations. Countries that commit to baseline privacy, due process, and human rights principles should be able to make direct requests to providers in other democratic countries. For other countries, existing mutual assistance frameworks should be reformed to improve response times.
Users' privacy rights are not adequately protected by current legal frameworks...	...Countries must commit to baseline principles of privacy, due process, and human rights in their domestic laws if they wish to make direct requests to providers in other democratic countries.

1. The Great Train Robbery of 1963 (and 2017)

In 1963, a train on its way from Glasgow to London was interdicted by a cohort of young men, who subsequently stole £2.6 million that they knew was being transported at the time. "The Great Train Robbery", as it became known, left an indelible mark on Britain as one of its most notorious crimes. The crime was meticulously planned and much of the stolen money was never recovered. Multiple investigations were launched using traditional investigative techniques at the time. Witnesses were interviewed, items were dusted for fingerprints, warnings about potential suspects were made to seaports, and most of the culprits were ultimately apprehended.

The investigation of a hypothetical Great Train Robbery in 2017 would involve some of the same investigative techniques used in 1963, but would also be different in significant ways. The availability of closed-circuit television (CCTV) footage could help identify the culprits and key witnesses. And the availability of data from email providers, social media services, communications services, and other providers could yield evidence identifying the culprits' whereabouts at the time of the crime and their communications about planning the heist.

And that's where things would get complicated. If a company in the United States (U.S.) provided an email service used to plan the robbery, the U.K. government would need to turn to the U.S. government for legal assistance to get the relevant emails. The U.S. might have grounds to open their own investigation, serve a warrant on the provider to get the emails, and then share them with U.K. officials. Absent the possibility of obtaining these emails from the U.S., the U.K. investigators would invoke a diplomatic process under the Mutual Legal Assistance Treaty[1] (MLAT) between the U.S. and the U.K.

MLATs are critical treaties that allow one country to seek assistance from another to obtain evidence and investigative support. The MLAT process serves an important function. It allows countries to cooperate in investigations, while ensuring that the values important to each are respected. The treaties respect the sovereignty interests of each country and allow even countries with largely adversarial relations to work together where there is common ground.

In recent years, however, the volume of MLAT requests submitted to the U.S. has swamped the system, which is largely a manual one. This growth in the number of requests is in large part because so many investigations involve evidence held by U.S. communications service providers. The volume combined with other factors such as lack of automation, poor understanding of what is required to be in an MLAT application to the U.S., and other challenges, has rendered the MLAT process slow and cumbersome. And so, the result is that today it may take many months before the U.K. government receives the communications content it sought. In the interim, the culprits would remain free, follow-on crimes may be committed, witnesses might move or become unavailable, and evidence could be destroyed. To reduce delays on its side, the U.S. may be able to expedite processing of the request, but of course that just comes at the expense of other pending requests that lose their place in the queue.

This state of affairs is untenable for governments with legitimate law enforcement interests. It leaves governments around the world looking for other ways to get the information they need for their public safety and security responsibilities. These alternatives can be unsavory, may cause collateral damage, undermine privacy and security protections for all of us, and may in the end be ineffective to get the information.

There is an urgent need for action to address these issues in a way that recognizes legitimate law enforcement interests, respects the sovereignty and political process of representative democracies, and lifts privacy, due process, and human rights standards throughout the world. In our view, such actions should:

- provide an alternative to MLATs for democratic countries to use to seek information directly from foreign providers;
- protect privacy based on who the user is, not based on where the data is stored; and
- modernize the MLAT process and implement other practical improvements.

The rules governing law enforcement access to data are becoming obsolete in two critical, but different ways. First, they do not ensure that countries with respect for the rule of law and human rights can obtain digital evidence – accessible and available in the cloud – in a manner that reflects the gravity of the law enforcement equities at stake. Second, they do not adequately protect the privacy rights of users in light of technological innovation. The adverse consequences of failing to update the law are now materializing – the result of mounting frustration from countries who are hampered in their ability to access digital evidence in a timely manner in order to prevent or investigate criminal and terrorist acts.

[1] | Treaty on Mutual Legal Assistance Between the United States of America and the United Kingdom of Great Britain and Northern Ireland, Signed at Washington on January 6, 1994 (online) www.state.gov/documents/organization/176269.pdf.

This is manifesting itself in the form of:

- the extraterritorial assertion of one country's laws in the face of clear conflicts of law;
- data localization proposals;
- aggressive enforcement efforts (e.g., imprisonment, substantial fines, garnishment of wages) targeted at employees of U.S. providers in countries outside the U.S; and
- proposals to enhance government access powers, including increased and aggressive government hacking efforts.

As concerns about crime and terrorism grow, we have seen proposals that would invariably create a conflict of laws between different countries. For example, as noted above, U.S. law generally prohibits U.S. companies from disclosing electronic communications content to foreign governments. As frustrations mount over the inability to obtain this data through sovereign channels in a timely manner, some foreign governments are resorting to other tactics – including the extraterritorial application of their own laws – that conflict with U.S. law.

Such conflicts between countries trying to protect their respective interests potentially put companies in the untenable position of deciding whether to risk violating the law of the requesting country or to risk violating the law of the country in which it is headquartered. Conflicts also significantly reduce the likelihood that law enforcement authorities will receive data from service providers, who become hamstrung in their ability to respond in light of such conflicts. It is in the interest of all stakeholders to work toward solutions that avoid conflicts of law, enable the production of digital evidence for legitimate law enforcement investigations, and incentivize the improvement of privacy and due process standards.

2. Two Fundamental Challenges

2.1. Governments Are Encumbered in Their Ability to Obtain Data for Legitimate Law Enforcement Investigations in a Timely Manner

Companies that provide communications services largely arose in a world where the services offered were for local users, and were mainly telephonic. Naturally and understandably, laws were created based on that reality. This factual assumption is reflected in the key U.S. laws, such as the Electronic Communications Privacy Act of 1986 (ECPA). ECPA has worked well for many years, and much of it remains vibrant and relevant, even in 2017. But it is also clear that some of its underlying technological assumptions are increasingly outmoded and ill-equipped to address a world in which data moves seamlessly and ubiquitously across borders. Understandably, the U.S. Congress in 1986 did not contemplate a world in which U.S.-based Internet companies would provide services to billions of users around the world. Because some of the biggest Internet communication service providers are located in the U.S., ECPA is a particularly important law, not just in the U.S., but throughout the world.

ECPA has created significant challenges in cross-border investigations where the production of digital evidence may be critical for solving or prosecuting crimes that take place outside of the U.S. ECPA contains a "blocking" provision that generally prohibits U.S. companies from disclosing communications content to foreign law enforcement agencies. In the absence of emergency circumstances, foreign governments – regardless of their adherence to baseline privacy, due process, and human rights standards – cannot receive communications content without relying on the MLAT process or other diplomatic channels, which often inhibit timely access to data for legitimate law enforcement purposes. In recent testimony[2] before the Senate and House Judiciary Committees, Paddy McGuinness, the United Kingdom's Deputy National Security Advisor, observed that this prohibition puts U.S. companies in the "invidious position of having to withhold information that could protect public safety".

Indeed, the blocking provision in ECPA is a source of enormous frustration for democratic countries that respect the rule of law and maintain substantive and procedural protection of civil liberties, and who need to investigate local

[2] | Written Statement of Mr Paddy McGuinness, Deputy National Security Adviser United Kingdom Before the Committee on the Judiciary House of Representatives, Presented on June 15, 2017, (online) https://judiciary.house.gov/wp-content/uploads/2017/06/McGuinness-Testimony.pdf.

crimes involving local users of U.S. services. In a letter[3] sent to the Presidency of the Council of the European Union, French and German Interior Ministers opined that "all too often, Member State authorities are faced with a refusal by service providers to provide information on legal grounds that we must be able to override. Electronic communication service providers must be able to contribute more to the successful outcome of investigations by being authorised to provide data linked to users' connections; in addition, data for European customers must be stored in a jurisdiction where direct cooperation with competent authorities of [EU] Member States is authorized". A recent French-British Action Plan[4] also calls for cooperation to "ensure that data and content of communications can be rapidly accessed for law enforcement across borders, wherever it is stored".

These countries are often unable to obtain timely access to digital evidence solely because it is retained by a U.S. service provider subject to ECPA, even for crimes that are wholly domestic in nature. The inability to obtain this data creates incentives for these countries to seek other techniques to get the information, including enforcement of their laws extraterritorially, even in the face of conflicting U.S. law. It also creates incentives for enactment of data localization laws and aggressive investigative efforts that undermine security in general and redound to the detriment of users' privacy.

The U.S. is not the only country with such blocking provisions. A recent survey[5] of the European Commission highlighted that the majority of European Member States' laws "do not cover/allow that service providers established in a Member State respond to direct requests from law enforcement authorities from another EU Member State or third country." In fact, it appears[6] that "only 2 Member States" allow for such cooperation. Such restrictions also exist for law enforcement authorities, who are often prevented by law from making requests for direct cooperation to service providers in any other country. It is quite clear that the challenges created by blocking provisions are international in scope and not merely confined to the U.S.

There are legitimate reasons that a country may wish to limit how a provider headquartered in its jurisdiction behaves, including to whom the provider discloses data. A country may, for example, want to prevent its local providers from disclosing the content of communications to governments with poor human rights records. A broad blocking statute that is divorced from policy implications and lacks nuance, however, can leave countries with a legitimate need for information looking for alternative means, some of which can be unsavory, aggressive, and unsafe.

> " Public safety and civil liberties should be improved through alternatives to diplomatic channels and procedures such as MLATs.

As discussed above, ECPA's blocking provision imposes a barrier to law enforcement agencies outside the United States and often prevents them from obtaining information held by U.S. providers, even where the agencies are in democratic countries that respect the rule of law and are investigating entirely domestic matters. Typically, such agencies will need to go through diplomatic channels with the U.S. government to obtain the content of communications. This can take many different forms, including letters rogatory and, where there is a treaty or executive agreement, through Mutual Legal Assistance Treaty (MLAT) requests. MLAT requests are a primary legal mechanism by which foreign governments obtain electronic communications content from U.S. service providers. MLATs enable foreign governments to request and obtain such

[3] | Council of European Union, Cover Note 14001/16, 7 November 2016, (online) http://data.consilium.europa.eu/doc/document/ST-14001-2016-INIT/en/pdf.

[4] | French-British Action Plan, published 13 June 2017, (online) www.gov.uk/government/uploads/system/uploads/attachment_data/file/619333/french_british_action_plan_paris_13_june_2017.pdf.

[5] | European Commission, "Questionnaire On Improving Criminal Justice In Cyberspace, Summary Of Responses" (online) https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf.

[6] | Ibidem.

communications content by making a request through the U.S. Department of Justice.

The MLAT process, however, is often slow and cumbersome. In part, this is because the number of MLAT demands have grown as evidence is more commonly held by companies in other jurisdictions, even if the crime itself is entirely local. In its 2015 Fiscal Year budget request[7], the Department of Justice noted that "[o]ver the past decade the number of requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs (OIA) has increased nearly 60 percent, and the number of requests for computer records has increased ten-fold. While the workload has increased dramatically, U.S. Government resources, including personnel and technology, have not kept pace with this increased demand." In 2013, the President's Review Group on Intelligence and Communications Technologies reported that MLAT requests "appear to average approximately 10 months to fulfil, with some requests taking considerably longer."[8]

The problem is not entirely with the U.S., however. The MLAT process is also often hindered by the requesting country's lack of understanding of what is required to satisfy U.S. legal standards, or inefficiencies in the system of the requesting country. These diplomatic channels are critical tools and need to work efficiently.

> "ECPA's limitations frustrate the U.S. government in its efforts to obtain user data in legitimate law enforcement investigations.

Out-of-date concepts in ECPA also plague government agencies in the U.S. A unanimous panel of the United States Court of Appeals for the Second Circuit held[9] last year that a search warrant issued under ECPA, as written, only permits U.S. government entities to compel a provider like Google to search for, seize, and produce records that are stored in the U.S. The ruling underscored the challenges of interpreting a 1986 statute and applying it to modern-day technological realities and cross-border law enforcement investigations.

At the time ECPA was passed, this limitation on warrants may have made some sense. Times, and more importantly networks, have changed since then. The limitation on ECPA warrants to data stored in the U.S. has presented challenges to law enforcement, which service providers appreciate. And it has spawned litigation in other parts of the U.S. This is not to criticize the Second Circuit's decision, which is based on well-established and long-held principles of statutory construction. Rather, it is to underscore the importance of Congressional intervention to update the law. The cases pending around the country have judges working to understand what Congress intended in this statute enacted in 1986, well before providers like Google and Facebook existed.

But these challenges can be best addressed only by the U.S. Congress. Rather than imposing limits under ECPA based on the location of data at the moment data is sought, a criterion applicable to traditional warrants, legal process under ECPA should be modified to consider the underlying user's nationality and location. Let's pay attention to the user, not to where the data is stored.

2.2 Users' Privacy Rights Can Be Improved

For many years, we have called upon the U.S. Congress to update the Electronic Communications Privacy Act (ECPA)

[7] | U.S. DOJ, „2015 Fiscal Year budget request", (online) www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[8] | Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 12 December 2013, p.229 (online) https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[9] | 14-2985 Microsoft v. United States, "Decision on the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation", 2d Circuit 2016 (online) https://tinyurl.com/yahgkkuu.

and codify a warrant-for-content standard[10]. As we noted in previous testimony before the U.S. Congress, a warrant-for-content standard is effectively the law of the land today. This standard is observed by governmental entities and providers alike and has been embraced by courts as necessary to satisfy U.S. constitutional standards. In 2016 and 2017, the House of Representatives passed the Email Privacy Act, which would codify a warrant-for-content standard. But it hasn't been enacted into law, despite the clear consensus that has emerged in support of this standard.

> “Any framework for cross-border law enforcement requests should establish baseline privacy, due process, and human rights standards.

Currently, some of the world's largest Internet companies are headquartered in the U.S. and thus subject to U.S. jurisdiction. Policy reform in the U.S., such as codifying the warrant-for-content standard, is thus critical to engender and incentivize the types of international reforms that can improve global privacy and due process standards while addressing legitimate law enforcement needs.

This is all the more important as many countries still lack such robust safeguards and standards for government access to data in the cloud. Even among like-minded countries, standards vary greatly[11], despite the fact that users' reasonable expectations of privacy vis a vis government access do not. A broader, international framework for cross-border law enforcement requests necessitates changes in the domestic statutes of countries that do not adequately protect privacy, due process, and human rights. This is core to any fundamental realignment of government access laws; it must reflect modern law enforcement needs and the privacy expectations and rights of Internet users.

This will undoubtedly require time and significant change for many countries. It also means that the MLAT process will be the primary mechanism that many countries will rely upon for the foreseeable future. However, adherence to baseline privacy, due process, and human rights standards are and should be no less compelling than law enforcement interests in obtaining electronic evidence stored in the cloud.

3. Proposed Solutions: A Blueprint for Reform

In debates about government access standards, there is an understandable tendency to view solutions as a balancing act, where improving governments' postures to obtain user data necessarily entails a trade off with user privacy (or vice versa as the case may be). But the goals of creating more efficient government access standards and stronger privacy and due process standards are not mutually exclusive. Indeed, by updating the law to reflect the new realities, we will be creating new approaches that are better for law enforcement and civil liberties. We can and should endeavor to achieve both without searching for a balance that necessarily suggests a trade-off.

The proposed solutions set forth below aim to address the two fundamental challenges outlined above. We believe these ideas can make significant progress towards addressing these challenges, but we also recognize that workable international frameworks will require input and contributions from a broader group of stakeholders.

> “The reform should enable certain democratic countries to obtain electronic data from U.S. service providers.

[10] Hearing on “ECPA Part 1: Lawful Access to Stored Content”, Written Testimony of Richard Salgado, House Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations, 19 March 2013 (online) http://judiciary.house.gov/_files/hearings/113th/03192013_2/Salgado%2003192013.pdf.

[11] Hogan Lovells, “Hogan Lovells White Paper on Governmental Access to Data in the Cloud Debunks Faulty Assumption That US Access is Unique”, 23 May 2013 (online) www.hldataprotection.com/2012/05/articles/international-eu-privacy/hogan-lovells-white-paper-on-governmental-access-to-data-in-the-cloud-debunks-faulty-assumption-that-us-access-is-unique.

It is increasingly clear that solutions complementary to MLATs must be developed to address the challenges to cross-border law enforcement investigations created by the advent of the Internet era. This is long overdue. Countries that commit to baseline privacy, human rights, and due process principles should be able to make requests to U.S. providers in serious cases without the intervention and participation of the U.S. government. Making such an avenue available would have the salutary effect of incentivizing foreign countries to raise their privacy and due process standards so that they can avail themselves of this new and more efficient process.

Such a framework would also have the ancillary benefit of giving citizens of those countries a real stake in the outcome of legislative processes that address government access to data. Currently, U.S. law often governs the circumstances under which the data of non-U.S. persons is disclosed to their governments. A German law enforcement agency seeking communications content about a German Gmail user, for example, would have to meet U.S. legal standards to obtain such data in most cases. Amending U.S. law to lift the prohibition on disclosing communications content to certain foreign governments in serious cases shows deference to the democratic processes of representative governments and their citizens, many of whom may prefer the privacy protections afforded under their domestic laws to those afforded under U.S. law.

In July 2016 and again in May 2017, the U.S. Department of Justice (DOJ) unveiled legislation[12] that would amend ECPA to authorize, but not require, U.S. providers to disclose communications content to foreign governments that adhere to baseline due process, human rights, and privacy standards. This legislation would authorize the U.S. government to enter into executive agreements with foreign governments that meet minimum requirements of substantive and procedural protection of rights. Under such agreements, a qualifying foreign government could make legal requests to U.S. service providers in certain types of criminal investigations involving serious crimes without going through diplomatic channels, such as the MLAT process. DOJ and the Department of State would be required to determine and certify that a country adheres to baseline privacy, due process, and human rights principles before U.S. companies could disclose the content to that country. Foreign governments would be required to afford reciprocal rights to the U.S. government in obtaining access to electronic data that a foreign country may prohibit service providers from disclosing.

The U.S. and U.K. governments are in the process of negotiating this type of agreement, the first of its kind. The U.K. for its part has enacted legislation to implement what are key components of this agreement, including a requirement that legal demands for communications content have a strong factual basis and are reviewed by a judicial commissioner that is independent of the UK government. The expectation is that other democratic countries with a commitment to privacy, due process, human rights, and the rule of law will be candidates for future bilateral or multilateral agreements.

A framework of this kind can help set expectations about the types of changes that foreign governments will need to make in order to satisfy baseline privacy, due process, and human rights standards. Providing a pathway for these countries to obtain electronic evidence directly from service providers in other jurisdictions, where such jurisdictions have no appreciable equity to block disclosure, will remove incentives for the unilateral, extraterritorial assertion of a country's laws, data localization proposals, aggressive expansion of government access authorities, and dangerous investigative techniques, which are ultimately bad for us all.

The changes to U.S. law described above will provide powerful incentives for foreign countries to update their government access statutes in ways that comport with baseline privacy, due process, and human rights standards. There is no international consensus about what concrete measures governments must take to meet such standards, but there are different models that can inform this undertaking.

First, the legislation unveiled by DOJ last year describes the types of human rights norms that other countries must

[12] | U.S. DOJ, Office of Legislative affairs, Letter addressed to the President of the U.S. Senate, 15 July 2016, (online) www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1.

observe to receive certification for the types of executive agreements that the legislation envisions. For example, countries must demonstrate "respect for the rule of law and principles of non-discrimination", and adhere to international human rights norms that include, but are not limited to "protection from arbitrary and unlawful interference with privacy; fair trial rights; freedoms of expression and peaceful assembly; prohibitions on arbitrary arrest and detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment." Legal orders from such governments must be "based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation". Such orders issued by foreign governments "must be subject to review or oversight by a court, judge, magistrate, or other independent authority".

Second, the Necessary and Proportionate Principles[13] can also be a useful lodestar. In 2013, the United Nations' Human Rights Council initiated a process to develop and articulate principles that governments could emulate in fashioning government access statutes that comport with international human rights law. The result of that process is the Necessary and Proportionate Principles, a set of thirteen guideposts developed by privacy and human rights non-governmental organizations across the world. The Necessary and Proportionate Principles – as the prefatory text notes – can provide governments with a "framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights."

Provided that countries can meet baseline privacy, due process, and human rights standards, the bilateral agreements authorized by the legislation unveiled by DOJ provide the most promising avenue to appreciably improve global privacy standards and create a pathway for foreign governments to obtain digital evidence for legitimate law enforcement investigations.

Of course, bilateral agreements are not the only path for improving privacy standards and enabling foreign governments to obtain digital evidence in legitimate law enforcement investigations. The same objectives may be better and perhaps more efficiently served through multilateral agreements that accomplish the same objectives. The current U.S.-U.K. agreement, however, is the best practical example thus far of addressing the various equities at stake. In light of the adverse consequences of inaction, it is critical that governments move quickly to address challenges that have been apparent for years and that are only growing more acute with the passage of time.

> " The International Communications Privacy Act should be enacted.

Relatedly, it is also critical that countries begin to refashion their domestic statutes to take into consideration the legitimate privacy interests of both individuals outside of their country and the comity interests of the countries in which those individuals are citizens. The International Communications Privacy Act (ICPA) is a framework that takes into consideration both of these equities. While we appreciate that ICPA will require refinements, it can be a useful model for other governments as they consider ways to adapt their domestic statutes to modern-day realities, where digital evidence is often vital to criminal investigations and often implicates the privacy rights of non-citizens and the comity interests of foreign countries.

Modern Internet networks increasingly store data intelligently, often moving and replicating data seamlessly between data centers and across borders in order to protect the integrity of the data and maximize efficiency and security for users. This technological reality underscores the importance of legislative solutions that eschew data location as a relevant consideration in determining whether a particular country can exercise jurisdiction over a service provider. Notably, all of the judges who issued pertinent rulings in the Second Circuit case (including both the original 2016 panel opinion and a 2017 ruling denying rehearing before the entire Second Circuit) urged Congress to consider appropriate changes to ECPA that would resolve

[13] | International Principles on the Application of Human Rights to Communications Surveillance, May 2014 (online) https://necessaryandproportionate.org/principles.

the policy questions at the heart of the case. Judge Lynch's concurrence in the 2016 case[14] is notable in this regard:

"Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised , with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations"[15].

Inaction means that important policy decisions about electronic privacy and government access fall by default to the courts. Courts are being asked to resolve individual disputes in ways that are divorced from sound policy solutions, without the robust opportunity for debate among a variety of stakeholders, and indeed potentially entirely in closed courtrooms. This is hardly the path for appropriately addressing the equities of users, law enforcement agencies, service providers, and foreign sovereigns.

The U.S. Congress has an opportunity to update ECPA for the Internet age, and to consider how the application of domestic U.S. government access laws affects the equities of foreign countries and the privacy rights of non-U.S. persons. A legislative framework that addresses the equities of relevant stakeholders is far preferable to a protracted litigation battle that is missing critical voices and perspectives. This is a job for Congress, not the courts. In the last Congress, Representatives Marino and DelBene, and Senators Hatch, Coons, and Heller, introduced the International Communications Privacy Act (ICPA). With some further refinements, ICPA can provide the right framework for cross-border law enforcement demands for user data. The following principles should inform further changes to ICPA. We believe it is important, however, to remain flexible in devising solutions to the broad array of challenges and wide array of equities at stake.

- **Warrants for Content:** Congress should codify a warrant-for-content standard. This has already passed the House of Representatives twice with no opposition, and this reform enjoys widespread support across the political spectrum.

- **Data Location:** Subject to the following additional principles, the location of data held by a U.S. provider should not in and of itself determine whether legal process issued under the stored communications chapter of ECPA can reach that data.

- **Notice:** When a government agency in one country endeavors to obtain, through lawful process, from a provider in its own jurisdiction, the electronic data of a user who is a national of or located in a different country, that agency should provide notice to that other country. There will be understandable exceptions and limitations to this notice requirement, but a country that has established diplomatic mechanisms (e.g., a Mutual Legal Assistance Treaty (MLAT)) with another country for the production of data in cross-border investigations, and that observes shared, baseline principles of privacy, due process, and human rights, should honor this notice principle. This affords the other country an opportunity to raise concerns, through diplomatic channels for example, about the request in light of the legitimate privacy interests of its citizens and the comity interests and values of that country.

- **Redress and Comity Factors:** A jurisdiction that receives the notice contemplated above should have the opportunity for redress in the requesting country's jurisdiction. This may include the opportunity to initiate a legal challenge in the requesting country's jurisdiction. Courts that hear such challenges should conduct a comity analysis to help weigh the equities of the countries. Factors to be considered under that analysis could include: (i) the location and nationality of the customer or subscriber; (ii) the location of the crime; (iii) the seriousness of the crime; (iv) the importance of the data

[14] Op. cit. 14-2985 Microsoft v. United States.

[15] Ibidem, p.63 (emphasis added).

to the investigation; and (v) the possibility of accessing the data via other means.

- **Reciprocity:** Countries that extend the aforementioned rights (i.e., notice and redress) to other countries under their domestic laws should expect reciprocity. Countries should not be required to provide notice or redress mechanisms to other countries that are not obliged to reciprocate. And no country, of course, should be required to extend the aforementioned rights to countries that fail to adhere to baseline privacy, due process, and human rights standards.

The basis for a legislative framework that addresses the various equities at stake exists, and we are eager to work with interested stakeholder to update ECPA in this manner.

Modernize the MLAT Process

There is no panacea for the range of challenges presented by aging legal regimes that are ill-equipped to address technological innovation, modern law enforcement needs, and strong privacy, due process, and human rights standards. MLAT improvements remain critical to instill confidence in the ability of the U.S. to provide data to foreign law enforcement agencies in a timely manner. The vast majority of countries are going to rely on MLATs and comparable diplomatic mechanisms for the foreseeable future, which underscores the importance of moving quickly to fully fund and implement the necessary reforms to the MLAT process. There are a number of ways that the DOJ could modernize its response procedures for MLAT requests.

- **Develop a Standard Electronic Form and Online Docketing System for MLAT Requests:** DOJ should create a publicly available, standardized online form for the submission of MLAT requests. Separately, DOJ should create an online docketing for receipt of MLAT requests accessible only to those MLAT partners. Foreign governments should be able to utilize this online docketing system to track the status of outstanding MLAT requests.

- **Streamline Review of MLAT Requests:** DOJ could streamline the handling of MLAT requests for content data by eliminating the need for duplicative review by both its Office of International Affairs (OIA) and a local U.S. Attorney's Office. This could be accomplished in multiple ways, using existing statutory authorities. For example, OIA attorneys could review the MLAT request, prepare the U.S. legal documents needed to execute that request, and file those documents directly with a U.S. court, without the need to work through a local U.S. Attorney's Office. Second, OIA attorneys could prepare the U.S. legal documents needed to execute the MLAT request and then provide those documents to an Assistant U.S. Attorney in the District of Columbia or another appropriate district who has been specially designated to file those documents on behalf of OIA. The second option would expand on a highly successful pilot project OIA recently conducted with the U.S. Attorney's Office for the District of Columbia for requests for § 2703(d) orders. Both options, which are not mutually exclusive, would significantly streamline the MLAT process by eliminating the delay caused by having multiple DOJ attorneys in different offices review and process the same MLAT request.

- **Engage Foreign Partners and Improve Training:** The Justice Department, in conjunction with other agencies, should keep an ongoing line of communication with their MLAT counterparts across borders and establish single points of contact so there is no confusion about where requests or orders should be sent. The U.S. government should also work to increase and standardize education and training of law-enforcement ministries, the U.S. judiciary, and other interested parties on how to utilize MLATs effectively. This will require further coordination with the U.S. Department of State, the Federal Bureau of Investigation's Legal Attache offices, and other relevant U.S. federal and private sector entities to host overseas training sessions at U.S. Embassies. These sessions could focus on best practices relating to the use of MLATs, applicable U.S. legal requirements such as probable cause, guidance on electronic forensics, and overviews of modern electronic data technologies relevant to criminal investigations.

- **Increase Transparency:** The Departments of Justice and State should work together to increase transparency and provide online and searchable treaty documents, compliance guidance, FAQ's, aggregate metrics, and other materials to international law enforcement and, where appropriate, to the public. This will improve the documentation available concerning the submission of MLAT requests and facilitate greater understanding of U.S. legal standards for foreign counterparts/agencies, which often struggle to formulate MLAT requests that meet the U.S. standard of probable cause. Providing this type of guidance in an accessible manner will contribute to higher-quality submissions to OIA, which in turn should help reduce review and processing time for those requests. In addition, public reporting on improved response times and other progress would increase trust by foreign law enforcement officials in the MLAT process as a reliable mechanism for law enforcement requests.

- **Increase Resources:** The U.S. government should allocate significant new resources to OIA in order to enhance its personnel and to implement the other recommendations outlined above for improving the MLAT process. Given its current constraints and the significant increase in volume of requests it handles, it is unreasonable to expect OIA fully address these challenges without a surge in personnel and other resources.

This is by no means an exhaustive list of policy options available to governments. Indeed, the Global Network Initiative's report, entitled "Data Beyond Borders — Mutual Legal Assistance in the Internet Age"16, provides additional recommendations for improving the MLAT process. Foreign governments should also consider practical ways to improve cooperation with U.S. authorities. For example, the European Commission's recent efforts17, which includes financial support for the exchange of best practices and training for EU practitioners on relevant U.S. law, is a good start. Foreign governments are often slowed by their own internal inefficiencies in transmitting MLAT requests to the U.S.

Develop Practical Solutions for the Near Term

Bilateral frameworks that can facilitate the production of digital evidence in cross-border investigations, while lifting global privacy standards, are undoubtedly ambitious undertakings. In the interim, there are practical steps that governments and service providers can take to make the provisioning of data in cross-border law enforcement investigations more efficient, which can help reduce the likelihood that governments will resort to more aggressive measures that will invariably weaken privacy and due process standards.

Based on our experience, there are meaningful and practical steps that improve cooperation between law enforcement and providers and help relieve some of the pressures of the problematic proposals described elsewhere in this document.

- **Single Points of Contact (SPOCs):** Law enforcement authorities should designate officials to serve as dedicated points of contact for working with foreign communication service providers. The officials would be responsible for understanding the legal requirements and know how to submit legal process to a provider, what to expect in return, and how to deal knowledgeably and quickly with errors and misunderstandings that inevitably arise. We have seen that such points of contact help ensure that the requests are appropriately formulated and facilitate verification by providers that the requests are authentic. It would also consolidate (and limit) the number of requests concerning the same investigation. SPOCs have achieved meaningful improvements in the effectiveness of cooperation in many countries that have adopted this posture, and this is a promising avenue for improving the MLAT process18 in other countries as well.

- **Train the Trainer:** International and regional organizations should work on consolidated train-the-trainer programs in which providers should participate. Such systems are particularly effective in systems where there are SPOCs as discussed above.

- **Clarity on Applicable Law:** International and regional organizations should work to collect, translate and keep up-to-date national legal requirements related to access to data, including both primary and secondary legislation. This would ensure that providers and authorities have a common understanding what these procedures and legal requirements are.

Conclusions

Government access laws are due for a fundamental realignment and update in light of the proliferation of technology, the very real security threats to people, and the expectations of privacy that Internet users have in their communications. This is not merely an aspiration, but a necessity.

If the current trajectory does not change, there will be an even more chaotic, conflicting world of expansive government access laws and overly-aggressive investigative techniques that will weaken privacy protections for users and exacerbate existing tensions between governments and service providers. This could undermine the global Internet that is driving economic and social progress around the world and would ultimately undermine cooperation between law enforcement authorities and service providers. We are confident that the solutions outlined above can accelerate the development of international legal frameworks that reflect sound policy judgments. ■

POLICY REVIEW

ALL ELECTIONS ARE HACKABLE: SCALABLE LESSONS FROM SECURE I-VOTING AND GLOBAL ELECTION HACKS[1]

LIISA PAST
is the Chief Research Officer of the cyber security branch of the Estonian Information System Authority. She is a cyber defense and strategic communication professional with proven track record in consulting, training and research across sectors induces a variety of commercial, NGO and corporate clients. Highlights of current work include teaching at several universities and leading two teams at the world's largest international technical cyber defence exercise Locked Shields.

“There's been a lot of claims that our election system is unhackable. That's BS. Only a fool or liar would try to claim that their database or machine was unhackable,” said Jake Braun of DefCon 2017 hacker voting village[2] where the participants successfully compromised a number of voting machines[3].

Like traditional paper ballots at a polling station, no electronic election technology is 100% secure 100% of the time. Just as with ensuring the uniformity, secrecy and integrity of the conventional voting process, a multitude of measures can be taken to prevent, detect, manage and mitigate risks of using election technology and, in particular, online voting. While the risks can be different from conventional paper ballots and thus require specific mitigation, they are not greater, as the Estonian experience has demonstrated through the past dozen years[4].

Electronic voting components are common in different election systems and can be defined as “use of electronic means to record, process, or tally votes”[5]. Internet voting is one of these technologies. Here and

[1] This piece is not sponsored by any entity and reflects the opinions of the author alone. The author's position as the Chief Research Officer of the Cyber Security Branch of the Estonian Information System Authority means she has been professionally involved in aspect of planning I-voting in the 2017 Estonian municipal elections and this analysis inevitably is informed by that experience.

[2] Reuters, Hackers Will Be Breaking Into Voting Machines This Weekend, 2017 [online]. Retrieved August 06, 2017, from Fortune: http://fortune.com/2017/07/28/russia-election-hacking-def-con.

[3] Newman L. H., To Fix Voting Machines, Hackers Tear Them Apart, 2017 [online]. Retrieved August 06, 2017, from Wired: www.wired.com/story/voting-machine-hacks-defcon/ ; Anderson, M., DefCon Hackers Found Many Holes in Voting Machines and Poll Systems, 2017 [online]. Retrieved August 06, 2017, from IEEE Spectrum: http://spectrum.ieee.org/tech-talk/computing/networks/defcon-hackers-find-holes-in-every-voting-machine.

[4] Author's interviews, e. a.-g., Interviews with election and e-governance officials, July-August 2017.

[5] Nurse J., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., Creese, S., An Independent Assessment of the Procedural Components of the Estonian Internet Voting System, Oxford 2016.

henceforth the terms "I-voting" and "online voting" are used interchangeably to mean the process of recording votes remotely using internet-connected computers. Some literature refers to I-voting as "e-voting," but unless in a direct quote, that term is generally avoided here to distinguish between use of electronic voting components (such as voting machines, electronic tallying etc.) and remote online voting.

Background: Global Election Hacks

Election technology has, in the past year, come to the focus because of increasing attempts, attributed to nation states or entities commanded by nation states, to influence elections and campaigns across the world. This "election hacking" denotes phenomena ranging from e-mail leaks and website defacement to compromising voter rolls or attempts to penetrate campaign finance or voting systems.

> " This "election hacking" denotes phenomena ranging from e-mail leaks and website defacement to compromising voter rolls or attempts to penetrate campaign finance or voting systems.

Often coupled with intense information operations, these cyber attacks on systems linked to campaigns and elections mean the adversary does not shy away from directly influencing the fundamental democratic processes of another nation. This has serious implications for liberal-democracies and how technology is used in the electoral process, what the security processes and standards should be and, perhaps most importantly, the political and legislative will to continue with and introduce new election technology initiatives across nations.

Through this adversarial strategy involving an intelligence-led and politically directed campaign, cyber attacks on elections are inherently integrated, combining, for example, cyber, influence, psychological, and information operations. Bill Priestap of the FBI's Counterintelligence Division makes it clear that "Russia's 2016 Presidential election influence effort was its boldest to date in the United States. Moscow employed a multi-faceted approach intended to undermine confidence in our democratic process. Russia's activities included efforts to discredit Secretary Clinton and to publicly contrast her unfavorably with President Trump. This Russian effort included the weaponization of stolen cyber information, the use of Russia's English-language state media as a strategic messaging platform, and the mobilization of social media bots and trolls to spread disinformation and amplify Russian messaging"[6].

The most prominent attacks on the US (2016) and French (2017) Presidential elections have most visibly targeted the campaigns and candidates. While there is no evidence that the vote recording or tallying might have been tampered with in the US[7] or in other nations, such attacks do undermine the voter confidence and the legitimacy of an elected government by sowing doubt in political players and the body politic. This, in turn, helps to possibly delegitimize elected leaders, their decisions, and the government.

To meddle in the internal affairs of a nation or at least attempt to influence electoral behavior, the electoral process need not to be compromised at all in these hybrid scenarios. It is sufficient to attack, for example, prominent political players or widely used (government) e-services to raise questions regarding the reliance on electronic solutions and the social, political and economic institutions supporting such digital ways of life.

[6] | Priestap B., Statement of Bill Priestap Assistant Director Counterintelligence Division Federal Bureau of Investigation Before the Select Committee on Intelligence United States Senate For a Hearing Entitled "Assessing Russian Activities and Intentions in Recent Elections", 2017 [online]. Retrieved August 06, 2017, from US Senate Select Committee on Intelligence: www.intelligence.senate.gov/sites/default/files/documents/os-bpriestap-062117.pdf.

[7] | Ibidem.

The efforts mounted during the 2016-2017 elections can also be groundwork for more advanced cyber attacks that could potentially impact electoral rolls or vote recording and tallying. Attempts to access state systems were identified in at least 21 US states in 2016 with data said to have been copied for mapping purposes or to plan future attacks[8]. Compromised voter registration and campaign finance systems were later reported in at least 39 states[9] with targets including election technology vendors[10]. The effects are real – claims of tampering with election technology led Venezuela to political unrest in August 2017[11].

It should be noted, however, that domestic and foreign attempts to influence elections have not been brought about by election technology. Rather, election technology has become another domain in which voters exercise their rights and therefore for those who wish to suppress or interfere with those rights to further their goals.

With proper security, logs, verification, auditing and other safeguards, election technology allows for detecting irregularities – be it network traffic characteristic to a DDoS attack or tampering with votes or databases – and therefore mitigating their potentially devastating impact. In the Venezuelan case, a technology vendor published claims of tampering with the explanation that the election system is designed to be "tamper evident and self-reports any attempt to interfere with it. This means that the system is designed to protect the votes from any manipulation and to immediately identify and alert of such an attempt"[12].

> “ Given its fundamental role in the functioning of a representative democracy, election technology needs to be viewed in the wider context.

While the focus of this analysis is election technology itself, rather than the attacks, including cyber and information operations, against campaigns and political players, these cases need to be reviewed and serve to highlight that election technology cannot be viewed, analyzed and secured in isolation. Given its fundamental role in the functioning of a representative democracy, election technology needs to be viewed in the wider context. Risk assessment, as well as management decisions and steps taken to manage and mitigate risks related to election technology, need to take a holistic view and view the whole process with the understanding that the entirety of a liberal democratic process is viewed as an attack surface.

Such a comprehensive view or risk management is particularly important, as a politically motivated or state-backed attacker in cyberspace can generally take a longer-term perspective (a system may be compromised over an extended period of time) and maintain suitable resources for using a range of techniques and technologies. This allows the attacker to go undetected and employ an opportunistic and reactive strategy.

Combining that and the highly integrated nature of attacks against elections and campaigns, means that

[8] | Tanfani J., Russians targeted election systems in 21 states, but didn't change any results, officials say, 2017 [online]. Retrieved August 06, 2017, from LA Times: www.latimes.com/politics/washington/la-na-essential-washington-updates-russians-targeted-election-systems-in-1498059012-htmlstory.html.

[9] | Riley M. and Robertson J., Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known, 2017 [online]. Retrieved July 31, 2017, from Bloomberg Politics: www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[10] | Fessler P., Report: Russia Launched Cyberattack On Voting Vendor Ahead Of Election, 2017 [online]. Retrieved August 08, 2017, from NPR National Security: www.npr.org/2017/06/05/531649602/report-russia-launched-cyberattack-on-voting-vendor-ahead-of-election.

[11] | Sanchez F. and Armario C., Showdown set in Venezuela as new assembly prepares for power, 2017 [online]. Retrieved August 08, 2017, from Washington Post: www.washingtonpost.com/world/the_americas/vote-tampering-claims-jolt-venezuela-on-eve-of-new-assembly/2017/08/02/511e5a16-77ec-11e7-8c17-533c52b2f014_story.html?utm_term=.21bde077ffc8.

[12] | Smartmatic, Smartmatic Statement on the recent Constituent Assembly Election in Venezuela, 2017 [online]. Retrieved August 05, 2017, from Smartmatic: www.smartmatic.com/news/article/smartmatic-statement-on-the-recent-constituent-assembly-election-in-venezuela.

a liberal democracy, if it is to succeed, needs to also take a holistic and comprehensive approach, encompassing strategic communication and democratic education as much as securing the technology. This, as demonstrated by multiple campaigns in 2016, includes improving the cyber hygiene, awareness, capacity building and operational security of political actors and candidates, allowing them to take a comprehensive approach that encompasses cyber security as well. While these factors will not be examined further here, they do need to be taken into account.

1. Remote Voting Technology Across the World

I-voting (or online voting) is fundamentally different from election technologies discussed so far. Estonia, the Netherlands, Canada and Australia have, among others, tested remote online voting[13]. Many nations, most notably Germany and Switzerland, use a remote ballot system by mail. Online voting generally mimics such remote voting. While approaches vary, the commonalities are:

- Identification: Voters need to be identified to access the voting system. Estonia uses a secure digital identity (further elaborated below) while several nations have experimented with distributing credentials through mail, e-mail or SMS message, all distinctly less secure. Others have relied on identification through online banking, creating dependencies on a private sector service. Whatever the identification scheme (including no compulsory identification), it is both a live dependency as well as a possible attack vector of elections, digital or otherwise.

- Legal framework and political will: an election organizer has to ensure that the legal requirements for elections (secrecy, universality, integrity, security etc.) are met across the voting platforms, be it voting online, at the voting booth or having access to the ballot box otherwise. Several nations have put online voting, sometimes after a trial, on hold until courts or the legislator offer legal certainty, or political parties come to a consensus.

- Security: an election organizer has to ensure that the security requirements are met on par with voting at the polling place when implementing a remote voting solution.

None of these issues are unique to elections but rather environmental. Security, identification, and legal frameworks are required for all e-services and ways of casting a vote, therefore online voting benefits from – and fits into – a wider ecosystem.

2. Factors Facilitating I-voting Based on the Estonian Experience

Estonia was the first country to introduce I-voting in 2005[14] and has followed a unique path where the votes can be cast online during the early voting period. With the municipal elections of October 2017 being the ninth chance to vote online in a dozen years, the proportion of online voters has plateaued at a third (31.3% at the 2014 European Parliament elections and 30.5% at the 2015 parliamentary elections), a steady increase from 1.9% in the first-ever I-vote in 2005[15]. In this time Estonia has "established a trust relationship"[16] with voters.

2.1 I-voting Framework

§ 60 and § 156 of the Estonian Constitution dictates that elections are "general, uniform and direct" with

[13] | Competence Center for Electronic Voting and Participation, World map of E-voting, 2017 [online]. Retrieved August 08, 2017, from E-Voting.CC GmbH - Competence Center for Electronic Voting and Participation: www.e-voting.cc/en/it-elections/world-map.

[14] | Nurse, et al., op. cit., p.2 ; Vassil K., Introduction, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015), Tartu 2016, pp. 1-13.

[15] | State Electoral Office, Republic of Estonia., Statistics about Internet Voting in Estonia, (n.d.) [online]. Retrieved August 05, 2017, from State Electoral Office, Republic of Estonia: www.vvk.ee/voting-methods-in-estonia/engindex/statistics
While published during the Estonian 2017 election period, this paper is written before the municipal elections and therefore does not include data for the October 15, 2017 vote. The Estonian State Electoral Office is expected to have most up-to-date data available on www.valimised.ee/en.

[16] | Nurse, et al., op. cit., p.12.

voting being secret[17] and all voting methods have to adhere to this standard. Early voting is no exception and the requirements are the same whether the voter is casting an absentee ballot at a designated pre-voting polling station, requesting a ballot box to their place of residence or I-voting[18].

I-voting opens for seven days (10th-4th day before election day) and mimics double-envelope (postal) voting "where the inner, privacy-providing envelope is replaced by encrypting the vote using the central system's public key, and the outer authenticity and integrity layer is provided by signing the vote cryptogram with the voter's ID card"[19]. The votes are only opened and tallied once the personal information (digital signature or "outer envelope") is removed[20] and that happens on an "offline and air-gapped server"[21].

2.2 Security Measures by Design

Since introducing I-voting in 2005, Estonia has not seen a single significant technical or security incident influencing voting outcomes[22]. In addition to the election procedures described above[23], the following principles have been followed:

> " Since introducing I-voting in 2005, Estonia has not seen a single significant technical or security incident influencing voting outcomes.

- Reliance on existing ecosystem, including for identification and authentication of voters: Estonia relies fully on the state-backed secure digital identity (either ID-card or crypto-SIM-card-based) to identify voters online and allow them to digitally sign the electronic double envelope used to cast the Internet vote. This live dependency, explored further in the ecosystem subchapter of this paper, cannot be removed unless the voter identification requirement as such is removed. Additionally, Estonia relies on a digital population registry as one of the bases for all e-governance.

- Repeat voting: An I-voter can re-vote as many times as they would like and only the latest vote counts, with a paper ballot taking priority over online vote[CITATION Int17 \l 1061].

- Procedural controls "defining the main manual activities and practices that election officials engage in"[24] are a core component of I-voting and documented in the election manual and security policy available (mostly in Estonian) on the elections website[25]. Estonia relies heavily on these procedures focusing on data integrity between parts of the system, access control and mechanisms for dispute resolution and system continuity[26]. Additionally, dispute resolution is designed to be fast, so as to not hinder the election process[27].

[17] | Constitution of the Republic of Estonia, 1992 [online]. Retrieved August 08, 2017, from President of the Republic of Estonia: www.president.ee/en/republic-of-estonia/the-constitution.

[18] | Heinsalu A., Koitmäe A., Mandre L., Pilving M., and Vinkel, P., Elections in Estonia 1992-2015, Tallinn 2016.

[19] | Heiberg S., Martens T., Vinkel P., and Willemson, J., Improving the verifiability of the Estonian Internet Voting scheme, [in:] The International Conference on Electronic Voting E-Vote-ID 2016, ed. M. V. Robert Krimmer, Lochau/Bregenz 2016, pp. 92–107.

[20] | Vassil K., Introduction, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-20015), Tartu 2016, pp. 1-13; Internet Voting in Estonia, op. cit.

[21] | Nurse, et al., op. cit., p.4.

[22] | Author's interviews, op. cit.

[23] | For a more detailed decription, see Internet Voting in Estonia. Retrieved August 07, 2017, from National Electoral Committee: www.vvk.ee/voting-methods-in-estonia/ ; Heiberg S., Martens T., Vinkel P., and Willemson, J., Improving the verifiability of the Estonian Internet Voting scheme, [in:] The International Conference on Electronic Voting E-Vote-ID 2016, ed. M. V. Robert Krimmer, Lochau/Bregenz 2016, pp. 92–107 ; Heinsalu A., Koitmäe A., Mandre L., Pilving M. and Vinkel, P., Elections in Estonia 1992-2015, Tallinn 2016.

[24] | Nurse, et al., op. cit. pp. 5-6.

[25] | Author's interviews, op. cit.; State Electoral Office, Republic of Estonia., I-vote Documentation Collection (E-hääletamise dokumendid), (n.d.), [online]. Retrieved August 08, 2017, from State Electoral Office: www.vvk.ee/e-haaletamine/e-dokumendid.

[26] | Nurse, et al., op. cit.

[27] | Author's interviews, op. cit.

- Constant feedback and improvement: While a more formalized lessons-learned structure would be desired[28], Estonian election organizers have shown flexibility and agility in constantly improving I-voting. The improvements have, amongst other input, been based on events and feedback, be it academic study, OSCE reports or heads-up from technology experts[29].

- Transparency measures have "had a noteworthy impact on building confidence and trust in the I-voting system"[30]. This "aggressive openness"[31] means that:

Estonia publishes most of the I-voting documentation on the elections website (with the main exception being materials that expose vulnerabilities).
Estonia publishes the source code of the I-voting software on the open-source coding platform GitHub starting from 2013[32]. As a security precaution, the uploaded repository is not used for further development but is the "up-to-date code used in elections"[33]. The 2017 code is to be published after testing.
Estonia invites feedback from the technology community and Estonia's volunteer Cyber Defense League[34] in addition to formalized testing.
Estonia makes election procedures public and observable and parts of the system audited, all meeting standards similar to voting procedures at a polling station[35].

- Vote verification allows confirmation of whether "vote was cast as intended"[36] and therefore enables detection when the computer had been compromised in a way that "changes the I-vote or blocks the I-voting"[37]. Verification through separate devices (in Estonia's case computer and smartphone) makes vote hijacking on a large scale more difficult[38].

- Estonia owns the software: Procured through a public tender, the Estonian election organizers own the I-voting software, allowing them to develop it as needed. The code base for Estonian I-voting is separate from the commercial products of the developer, thus mitigating the risk of another customer discovering, withholding and exploiting vulnerabilities.

- Testing: a public dummy demonstration is used as a functionality test about a month before Election Day. Security/penetration testing is to be carried out as new software is introduced.

- Traffic monitoring: CERT_EE, the body responsible for managing security incidents in the .ee domain, is engaged in the I-voting task force and monitors the network traffic to detect any anomalies, including possible DDoS attacks. Tools and ways to monitor logs are also constantly improved and developed.

While voting in a location outside of the polling station without the presence of polling workers does create risks, majority of the user-caused risks are not scalable and the procedures and safeguards described mitigate those risks. Additionally, the agencies involved put an effort into cyber hygiene awareness raising to remind voters of proper use of digital identity (for example: do not share your pin codes, use trusted computers).

Fundamentally, I-voting taking place in the pre-election period offers a time buffer that allows for reverting to universal paper vote on Voting Day should the remote voting not meet standards or incidents occur. While

[28] | Nurse, et al., op. cit.

[29] | Author's interviews, op. cit.

[30] | Nurse, et al., op. cit., p. 3.

[31] | Author's interviews, op. cit.

[32] | I-voting on GitHub. Retrieved August 04, 2017, from Github: https://github.com/vvk-ehk/evalimine ; Internet Voting in Estonia. Retrieved August 07, 2017, from National Electoral Committee: http://www.vvk.ee/voting-methods-in-estonia.

[33] | I-voting on GitHub, op. cit.

[34] | For more see www.kaitseliit.ee/en/cyber-unit.

[35] | Author's interviews, op. cit.

[36] | Vassil, op. cit., p. 10.

[37] | Internet Voting in Estonia. Retrieved August 07, 2017, from National Electoral Committee: www.vvk.ee/voting-methods-in-estonia.

[38] | Nurse, et al., op. cit.

unlikely, the procedures (including availability of sufficient number of paper ballots and staffing at polling stations as well as legal procedures) are in place for such an eventuality[39]. This also highlights that the reasonable way to approach I-voting is to see it as an option, allowing voters a diversity of choices, rather than the only way to collect votes.

2.3 Comprehensive Risk Assessment

In the past, the risk assessment of the I-voting systems had focused on the threats under the direct control of the election organizers (including technical risks stemming from the software). Given the changed threat landscape and adversary's hybrid tactics, a more comprehensive risk assessment approach was introduced in 2017 to be able to mitigate risks arising from third parties and world politics as well as the lively digital ecosystem encompassing both Estonian e-governance solutions (including ID-card, population registry etc.) as well as third parties involved in the development and distribution of these solutions.

This is particularly important, as the legitimacy of the elections does not only depend on the technical execution of voting procedures. This approach also accounts for and suggests ways of mitigating risks arising from information/hybrid attacks, dependencies on the ecosystem, management issues, introducing new online voting software, the impact of a large group of first-time voters (for the first time, Estonia invites 16-18-year-olds to the polls) and other factors outside the direct control of the election organizers. The assessment includes dependencies on outside systems and services as well as ways to identify, manage and mitigate them, including approaches to transparent communication.

It is hoped that such a comprehensive approach, particularly as it was introduced early in the planning period, allows prioritization of tasks and resources according to their potential impact. The shared understanding of landscape brings parties involved to the same page in planning and management terms, thus allowing for better responses to eventualities as they arise

2.4 Reliance on Existing Ecosystem

I-voting in Estonia is facilitated by a lively ecosystem on government e-services and a secure digital identity that all Estonians and residents carry.

The ID-card is the fundamental live dependency of I-voting, similar to identity documentation in voting at a polling station The smart-card/chip-and-pin-based government-backed digitally usable identity document is supplemented by mobile-ID, a SIM-card based solution with equal guarantee. An additional electronic-use-only card is also available.

Digital ID identification/authentication is used to identify the voter online and allow them to cast and sign their vote[40]. Card readers are widely available at a reasonable price. They are a standard feature on new computers and common in public and office workstations. The procedure of voter identification during I-voting is described in detail on the website of the Estonian elections[41].

Voter rolls, alike other personalized e-services are based on the Population Register, the uniform government database of primary personal data "such as the name, address and personal identification code" of citizens and legal residents[42]. The register incudes documents related to the Family Act and residence and is interlinked with and draws upon numerous government e-services[43].

Estonia's legal framework is "designed to work seamlessly with the technological solutions of e-government"[44]. A robust data exchange layer or "middle-ware system" (the "x-tee" or x-road) seeks to "minimize repetitive data collection, improve interconnectedness of the state's

[39] | Author's interviews, op. cit.

[40] | Internet Voting in Estonia, op. cit.

[41] | Ibidem.

[42] | Republic of Estonia, Population Register from July 2017 on IT and Development Centre of the Ministry of the Interior.

[43] | Ibidem.

[44] | Vassil K., The Estonian e-government ecosystem, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten years (2005-2015), Tartu 2016, p.18.

database and avoids the time-consuming dealing with paper data entry and verification"[45]. This digital public administration lays groundwork for all government e-services, I-voting included.

> I-voting in Estonia is facilitated by a lively ecosystem on government e-services and a secure digital identity that all Estonians and residents carry.

The voter database therefore does not need to be prepared separately. Instead, the Population Register has an up-to-date database of those eligible to vote in particular elections and the "electronic lists of voters shall be sent to the State Electoral Office not later than by the thirteenth day before Election Day"[46]. Providing the voter lists in good time before voting procedures also means there is no live reliance on the Population Register and problems with or attacks against the database will not influence I-voting.

These interconnected solutions create an ecosystem allowing I-voting, and it would be difficult to even conceptualize it without the described elements. At the same time, the reliance on these services creates a critical dependency for I-voting. In the case of the digital identity, the dependency is necessarily a real-time live one that can be mitigated but not overcome. Whatever model of identification and authentication voting uses becomes a critical dependency for the availability of voting.

2.5 I-voter Is an Average Voter

"For the first three elections multiple socio-demographic, attitudinal, and behavioral factors had a non-trivial association with being a first-time e-voter. However, from the fourth election onward, the importance of these factors gradually diminished, indicating the diffusion of e-voting among the Estonian electorate"[47].

In Estonia, the I-voter does not differ from the statistically average voter in almost any way and no socioeconomic factor (gender, income, education or nationality) predicts online voting[48]. Even "computer literacy is no longer a clear driver of e-voting and thresholds set by modest skill level can over time be overcome with handily designed e-voting systems"[49].

Political preferences play no significant role in predicting participation in I-voting[50] meaning that, contrary to popular belief, no political party or their voter base is (dis)advantaged by I-voting. Once normalized, the only predictor of I-voting is the distance to a polling station, as the technological solution offsets the cost of voting. "The critical limit is a 30 minute round trip to the ballot station, anything above that makes e-voting already more probable than voting at the polling station"[51].

Most recent research based on Estonian data suggests I-voting "to be very "sticky"; a first time e-voter is very likely to stay e-voting in subsequent elections at consistently higher rates than a typical paper voter is to stay paper voting, or a non-voter to remain a nonvoter"[52]. As a result, the potential of I-voting in boosting turnout remains to be explored, with the potential clearly outlined.

[45] | Vassil K., The Estonian e-government ecosystem, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten years (2005-2015), Tartu 2016, p.15.

[46] | Republic of Estonia, Riigikogu Election Act from June 2002.

[47] | Vassil K., and Solvak M., Diffusion of e-voting in Estonia, 2005-2015, [in:] E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015), Tartu 2016, p.67.

[48] | Vassil K., Solvak M., Vinkel P., Trechsel A., Alvarez R., and Hall T., Diffusion of Internet Voting: Usage Patterns of Internet Voting in Estonia Between 2005-2013, 72nd Annual Midwest Political Science Association Conference April 3-6, Chicago 2014; Vassil K., and Solvak M.(a), Diffusion of e-voting in Estonia, 2005-2015, [in:] E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 – 2015), Tartu 2016, pp. 57-70.

[49] | NVassil K., and Solvak M. (a), op. cit., p. 65.

[50] | Vassil K., and Solvak M. (a), op. cit., p. 69.

[51] | Solvak M., E-voting and the cost of electoral participation, [in:] E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015), Tartu 2016, p. 115.

[52] | Solvak M., and Vassil K. (b), Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming. Policy & Internet, 2017.

3. Scalability and Best Practice

Estonia serves as a case study and potential testing ground for e-services and digital government solutions as "smaller countries with strong institutions can create high value as early adopters and create a demonstration effect for the world by assembling the right ecosystem"[53]. This section looks at measures beyond the descriptions above to offer suggestions that would scale to larger societies seeking to protect election technology or introduce I-voting.

These measures focus on the social, legal and governance aspects and do need to be supplemented by both sound technical basis as well as a comprehensive risk management as described above. The Estonian strategy of transparency and publication of documentation serves a security purpose, supplementing risk assessment (including mapping of dependencies), clear procedures, testing and security by design. The Estonian approach is described above, with best practices outlined. Almost all the security precautions of I-voting are scalable to larger systems.

3.1 Start Small, Start Slow

The Estonian solution is particularly fitting in societies with few legacy systems and a lively ecosystem of (government) e-services, basic information infrastructure for secure electronic identity, and a national secure data exchange layer to facilitate communication between the systems listed above. As governments might move in that direction, their e-services cannot exist in isolation. In Estonia's case, "the involvement of private banks was pivotal with regard to the success of the ID-card, both regarding societal awareness and the actual distribution of cards"[54]. As the banks relied on the ID-card infrastructure to identify and authenticate their clients, it built trust and formed habits of using online services with the government-backed digital ID. For countries where such ecosystem is not as fully developed, focusing on a basic level of services and information infrastructure would be advisable before introducing I-voting.

> “ I-voting in national elections is a monumental task and governments would be well advised to start small, either with non-binding polls, or with provincial elections.

Similarly, I-voting in national elections is a monumental task and governments would be well advised to start small, either with non-binding polls, or with provincial elections. This also offers potential for dispersed populations, whether nations with large diaspora or tribal elections in sparsely populated areas[55]. A gradual approach allows for streamlining the process, and builds up trust at the heart of citizens' willingness to adopt I-voting that forms habits.

A gradual process ensures that I-voting and other election innovation is built to supplement the paper ballot voting, not at its expense. The paper ballot is fundamental to elections and will remain an advisable backup because "paper gives election officials a way a deliver a correct results"[56] in case of technology failures.

"Due to its slow take-off pace at the beginning," governments adopting election technology should allow time to assess the progress and potential[57]. The Estonian experience is most encouraging, as it took only three

[53] | Chaturvedi R., Bhalla A., and Chakravorti B., These are the world's most digitally advanced countries, 2017. Retrieved August 07, 2017, from World Economic Forum: https://www.weforum.org/agenda/2017/07/these-are-the-worlds-most-digitally-advanced-countries.
[54] | assil K., The Estonian e-government ecosystem, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten YEars (2005-2015), Tartu 2016, p. 24.
[55] | [CITATION Anu17 \l 1061].
[56] | Schurmann C., and Kickbusch J., Voting Machine Hackers Have 5 Tips to Save the Next Election, 2017. Retrieved August 06, 2017, from Wired: www.wired.com/story/voting-machine-hackers-5-tips.
[57] | Vassil K., Introduction, [in:] E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015), Tartu 2016, p.4.

elections for I-voting to fully diffuse. It is sometimes also hoped that I-voting would increase turnout by making voting easier[58]. The Estonian experience reaffirms that while technology can enable political participation, it does not remove other barriers to participation[59]. Thus governments are best advised to introduce technology hand-in-hand with other voter inclusiveness measures, not instead of them.

3.2 Comprehensive Approach and Stakeholderism

Given modern threats, including hybrid attacks against elections and the fundamentality of elections to citizens' rights, election technology and I-voting benefit from a comprehensive and cross-government approach. The discussion of risk management above showed that, as the target of the attacks is the legitimacy of a democratic process, detection and mitigation has to draw on a comprehensive toolbox of measures far wider than just technical tools to defend the democratic process and its participants.

Simply put, the planning assumption needs to be that the adversary will make all or any attempts to delegitimize a democratic process and its participants. Therefore, election organizers need to accept and mitigate or prepare for risks that are outside their control, such as e-mail leaks or website defacements or attacks against vendors and work with all stakeholders and possible targets to mitigate those risks.

> "Given modern threats, including hybrid attacks against elections and the fundamentality of elections to citizens' rights, election technology and I-voting benefit from a comprehensive and cross-government approach.

Secondly, functioning of elections cannot be up to only the elections organizers tasked with the technical execution. A multi-stakeholder approach, where all those involved in the electoral process have to be on board, means coordination and integrated (communication) management. In Estonia, for example, I-voting is managed by a task force that brings together the election organizer, the Information System Authority, the service providers I-voting relies on, and the software developer[60]. Communication is managed by a team comprising of representatives of the election organizer, the government office and, in the case of I-voting, the Information System Authority.

Regardless of their particular approach, all governments and election authorities need to constantly monitor and account for the ever-changing threat landscape. Lawrence Norden, co-author of the "Securing Elections From Foreign Interference" report by New York University School of Law's Brennan Center, said, "Threats are moving so much more quickly and I think that hasn't really sunk in for a lot of people"[61].

[58] | Vassil K., and Solvak M. (a), op. cit., p. 57.

[59] | Vassil K., and Solvak M. (a), op. cit., pp. 57-70.

[60] | Estonian National Electoral Committee, Riigi Teataja from June 2017 on Organization of I-voting (Elektroonilise hääletamise organisatsiooni kirjeldus).

[61] | Newman L. H., Securing Elections Remains Surprisingly Controversial. Retrieved August 07, 2017, from Wired: https://www.wired.com/story/election-security-critical-infrastructure.

Therefore there is a need to be well resourced, agile and flexible enough for systems and practices to be developed as new threats and attack vectors emerge.

In addition to functionality and security testing, outside critics and hackers can be embraced by election organizers to test election technology. For example, the Los Angeles County administrators took active interest in the DefCon hacking conference in July 2017 by planning to "invite the hackers to attack the proposed system as a test down the line – to 'kick the tires'", as part of a wider effort to redesign the electronic elements of voting[62].

These additional testers provide an extra pair of eyes, likely to discover or confirm vulnerabilities. As no testing methodology replicates another one, strength can play out in numbers. As security researcher T.J. Horner explained at DefCon, commercial testing might not be "as thorough or as public as the work" done at the hacker conference we did at the village"[63]. Therefore, it is important "to have a really broad range of people, a broad community, looking at this kind of technology if you have any hope of wanting to trust it to do something serious"[64].

3.3 Transparent Risk Management

Risks and vulnerabilities need to be openly addressed in public communication as the illusion of absolute security will undermine the election process as the first incident inevitably takes place. It often means communicating risks and vulnerabilities of technology, however theoretical, to an audience that is more accustomed to judging outcomes. In Estonia in 2017, a theoretical security vulnerability arising from the ID-card firmware became known to the Information System Authority about six weeks before the elections and just over a month before I-voting[65].

This vulnerability, while theoretical, impacted more than half of all ID cards in circulation[66]. While I-voting is also possible using the state-backed but less common mobile-ID and digital-ID, the risk, if materialized would have an instantaneous effect on I-voting, given the live dependency on the digital identity scheme. In addition to mitigating the potential risks and fixing the vulnerability, the authorities involved opted for open and transparent proactive risk management strategy where civil service, decision makers, international partners, the media, and the public were informed of the vulnerability as well as the risks involved, the steps to overcome. This included a cross-government communication approach, cooperation between agencies, cooperation with the appropriate international agencies and corporations, etc.

3.4 Documentation and Procedures

While Estonia has established sufficient and fast dispute resolution and "crucial procedures are clearly documented"[67], "sustainability of existing security procedures, particularly with reference to knowledge definition and transfer"[68] is considered problematic. Furthermore, Estonia's small committed staff means that those involved "already know what to do," as an interviewee said[69], and "in some cases incidents and feedback reports appear to be addressed in a somewhat informal way"[70], thus creating a potential sustainability and replication issue.

These risks can be mitigated by added procedural formality and thorough documentation, including in organizational (including roles, cooperation formats) and technical details (including routines, configurations). Such lessons that are learned, including incident handling

[62] | Leovy J., Worried about election hacking, L.A. County officials are turning to hackers for help. Retrieved August 06, 2017, from http://www.latimes.com/business/technology/la-fi-defcon-voting-20170724-story.html.

[63] | Newman L. H., To Fix Voting Machines, Hackers Tear Them Apart. Retrieved August 06, 2017, from Wired: https://www.wired.com/story/voting-machine-hacks-defcon.

[64] | Matt Blaze, professor and director of the University of Pennsylvania's Distributed Systems Lab, added at DefCon [CITATION Bar17 \l 1061].

[65] | Estonian Police and Border Guard Board with Estonian Information System Authority from September 2017 on Possible Security Vulnerability Detected in the Estonian ID-card Chip.

[66] | Ibidem.

[67] | Nurse, et al., op. cit., p.3.

[68] | Nurse, et al., op. cit. p.6.

[69] | Ibidem.

[70] | Nurse, et al., op. cit. p.11.

and other documentation would make the process less dependent on seasoned professionals and add clarity to planning, which would better allow for preparation for expectancies as well as the allocation of resources.

The same routines, to a great degree, mitigate human risks, including reliance on a single individual and the possibility of an insider threat. In the Estonian case, insider threats "may be unlikely given the relationships and professional trust"[71], but it should not be overlooked. For larger nations, comprehensive documentation is useful in addition to advanced vetting of personnel and further security procedures.

3.5 Voter Education

The voter is generally viewed as "the most vulnerable link in the I-voting system"[72], and Estonia has taken a number of measures have been taken to mitigate this. Voter education cannot focus on the particular technology (I-voting happening less than once a year does not incentivize specific leaning) but rather basic cyber hygiene.

> " Voter education cannot focus on the particular technology but rather basic cyber hygiene.

Awareness is a key factor in building trust in the system, therefore driving habit formation. In addition to the "significant amount of detail on the system online"[73], wider voter education campaigns are needed. Uninformed voters will not adopt the I-voting technology or, as Cybernetica (the provider of Estonian I-voting software) highlights, voters' lack of awareness of their responsibility for the safe conducting of the voting procedures[74] contributes to risks in carrying out the election procedures.

Education becomes particularly important with less tech-savvy voters. Those least likely to participate in elections are also those least empowered to use I-voting, as research by Mihkel Solvak highlights[75]. The solution, therefore, would be promoting basic computer literacy and hygiene rather than promoting I-voting by itself.

3.6 Legal framework

"Legislative efforts which typically follow technological developments are fundamental for the adoption and implementation"[76] of voting technology. As election technology is expanding an existing practice of exercising democratic rights into a new digital domain, the legislator and courts will need to test the constitutionality of election technology to prove that they meet the legal standards and requirements for free and fair elections. The language varies somewhat nation-to-nation, but any voting mechanism will need to meet the requirements of general, uniform and direct elections with the individual vote being secure. The organizer of the elections has to assure the voter's freedom to cast their vote as preferred as well as transparency, accountability (including correct tallying with appropriate auditing, verification and observation processes in place) and public confidence in the elections.

Similar to any information system or network, the confidentiality, integrity and availability of election technology and data can only be assured if resources are available, including competent staff and sufficient funding. In many ways, therefore, voting technology is not unique and governments are empowered to make sure the process is secure, whether electronic or on paper.

However, given the fundamental importance of elections in a democracy, governments might wish to set clearer standards in wishing to ensure the security of electoral process. This can be done by implementing baseline security standards (including appropriate reporting and auditing) or designating elections, voting, or services

[71] | Nurse, et al., op. cit. p.6.

[72] | Nurse, et al., op. cit. p.7.

[73] | Nurse, et al., op. cit. p.9.

[74] | Heiberg S., and Willemson J., Modelling Attacks Against I-Voting (Elektroonilise hääletamise vastaste rünnete modelleerimine), Tallinn 2011.

[75] | Solvak M., Mobilization, [in:] E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015), Tartu 2016, p.105.

[76] | Nurse, et al., op. cit., p.11.

elections rely upon (population databases, digital identity) and connection between these elements as critical information infrastructure or essential service. In some nations, local legislation might foresee other mechanism to mandate thorough security standards. Regardless of the approach, these measures are only effective if married to resources to properly implement them.

"Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law," the former US Secretary of Homeland Security, Jeh Johnson, has argued[77]. The definition of "election infrastructure" in this context is a comprehensive one: "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments"[78].

While such moves in the US have been met with some criticism as possible federal overreach, the DHS outlines that the move prioritizes federal efforts, makes security expertise and funding available, and improves communication and information-sharing between the stakeholders (including federal and state entities) on threats and vulnerabilities[79].

The US is by no means alone, even if national governments furnish critical infrastructure and essential services in a variety of ways. Among EU member countries, the transposition of the Directive on security of network and information systems (NIS Directive) might offer an opportunity to review the issue. While the directive focuses on the single market and does not list elections or voting as an essential service (for the list see Annex II, for definitions and identification Articles 4,5 of the directive), national governments have the freedom to furnish the transposition. The attacks on elections and related systems of 2016-2017 seem to have provided momentum for several European governments to consider it.

These steps might also carry symbolic value as these mechanisms highlight the sort of "benefits and protections" election technology enjoys[80]. This means national governments can provide support and resources thus signaling the commitment and potentially contributing to deterrence against election meddling.

Conclusion

In conclusion, election technology, particularly I-voting, can be introduced and promoted with a comprehensive cross-government view with awareness of the complex threat landscape. It is shortsighted to view I-voting or any other election technology as a technical process, as it is a fundamental part of exercising democratic rights. Therefore, the protection and constant legitimization of the democratic process itself has to be at the center of election innovation. For example, new voting technology should not and need not be introduced at the cost of neglecting conventional paper ballots, and election technology cannot exist in isolation.

Estonia is a case study of a realistic, scalable ecosystem of e-services that fosters I-voting and could support election technology. The ecosystem needs to include a wealth of digital services from government and private sector to build trust and form habits. In particular, a government-backed secure digital identity, robust data exchange layer facilitating e-services, and a reliable population register all create conditions for I-voting.

[77] | US Department of Homeland Security, Statement by Secretary Jeh Johnson from January 2017 on the Designation of Election Infrastructure as a Critical Infrastructure Subsector.

[78] | Ibidem.

[79] | US Election Assistance Commission on Starting Point: U.S. Election Systems as Critical Infrastructure (Whitepaper); US Department of Homeland Security from 06 January 2017 on Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector; Newman L. H., Securing Elections Remains Surprisingly Controversial. Retrieved August 07, 2017, from Wired: https://www.wired.com/story/election-security-critical-infrastructure.

[80] | US Department of Homeland Security, op. cit.

> “Estonia is a case study of a realistic, scalable ecosystem of e-services that fosters I-voting and could support election technology. The ecosystem needs to include a wealth of digital services from government and private sector to build trust and form habits.

For a number of states grappling with declining turnouts at elections and with concomitant worries about the security of I-voting and governmental electronic services, the Estonian case provides a timely and useful study that attempts security-by-design whilst recognizing that residual risks will remain and needs careful checks and balances at micro and macro levels with attendant issues of scalability, including those of human-technical resources.

Acknowledgments

I would like to thank my colleagues at the Estonian Information System Authority, Kadri Kaska in particular, as well as Priit Vinkel and his team of the Estonian State Electoral Office and Dr Kristan Stoddart of Aberystwyth University. Your remarks have been invaluable. Similarly, the editors of this Journal have been most constructive and graceful during the writing process. ■

ANALYSIS

WHAT CAN WE LEARN FROM WANNACRY AND NYETYA?

LOTHAR RENNER
leads Cisco's Security business in Eastern Europe, Russia / CIS and Switzerland. He is responsible for creating and delivering the security strategy and driving sales growth. He oversees more than 28 countries with an emphasis on keeping customers secure in an increasing threat landscape. Lothar and his team engage with hundreds of leaders in the enterprise, public sector, service provider and partner led markets, enabling them to transform organisations with innovative technologies from Cisco. Prior to leading Cybersecurity, Lothar led the Services business for Central Europe. Lothar joined Cisco 19 years ago in Germany. He has held numerous leadership positions in Cisco in Germany and Central Europe.

Back in May this year, WannaCry marked the beginning of a new era of ransomware. It spread like wildfire across the globe, faster than any ransomware attack ever seen before. Less than two months later, the world was facing another major cyber attack. Nyetya (or Petya) was destructive in nature and not economically motivated. It also spread fast, but used different methods. Yet these two events had one thing in common: their great scale and destruction. At Cisco, our threat intelligence team Talos even invented a name for these threats, calling them destruction of service attacks. Far more damaging than earlier attacks, they may leave businesses with no way to recover.

> “We live in a hyper-connected world, and as connectivity grows, so does the potential for large-scale attacks.

We live in a hyper-connected world, and as connectivity grows, so does the potential for large-scale attacks. Technology, such as the Internet of Things, is no longer an idea for the future; it is already here. More and more companies are digitising their operations; more devices are being connected to the networks. The benefits are huge, but they don't come without risk.

Cyberattacks are a fact of life, but companies and organizations can improve their security posture and soften the impact. Here are a few lessons we learned about how the threat landscape is evolving and what you can do to protect your organisation.

WannaCry: Anatomy of the Attack

On 14th March 2017, Microsoft released a patch (MS17–010) for a new SMB vulnerability. While this protected newer Windows computers that had Windows Update enabled, many computers remained unpatched globally. This is particularly true of Win XP computers which were no longer supported by Microsoft, as well as the millions of computers globally running pirated software, which are (obviously) not automatically upgraded. As a result, in May 2017, WannaCry infested hundreds of thousands of unpatched devices in more than 100 countries, making it the biggest ransomware outbreak to date. Such notable organisations like the National Healthcare Service in the UK, Telefonica in Spain and Deutsche Bahn in Germany were among the targets.

On 12th May, MalwareTechBlog released the information about the attack and how to shut it down. A screenshot of Cisco investigation was included in the post and used as a part of the intelligence collection and discovery.

Ten minutes after the “kill switch” domain became public, we had already added it to the Cisco Umbrella list of “newly seen domains”. What this domain actually does is that it stops infected computers from completing the encryption. It doesn't remove the ransomware, but it renders it useless.

Sixty minutes later, the WannaCry ransomware attack reached some of our customers and Cisco Advanced Malware Protection (AMP) automatically blocked those samples. Less than 3 hours after the WannaCry outbreak was first noticed, it was already officially listed as malware in all Cisco solutions, protecting our customers.

Long before WannaCry terrorised companies everywhere, we had already addressed the vulnerabilities that this type of ransomware worm exploited to get into so many computers. Cisco Talos – a global threat intelligence organisation with over 250 world-class researchers and a network of global intelligence and data resources – released SNORT signatures to help identify the MS vulnerability back on the 14th March, the same day that Microsoft released the patch. On 25th April, Cisco Talos released additional SNORT signatures for Double Pulsar and anonymous SMB shares, addressing the vulnerabilities released by Shadow Brokers on the 14th April. Companies that patched these vulnerabilities on their computers before 12th May were immune from WannaCry infection.

Nyetya: Ransomware Continues to Make the Headlines

Six weeks later, another variant of ransomware attacked multiple organisations in several countries. Cisco Talos actively investigated it and named in Nyetya. This new ransomware variant encrypted the master boot record (MBR) of a system, comparable to the table of contents for the hard drive – clearly very important. Once this ransomware entered the system, it used three ways to spread automatically around a network, one of which was the known Eternal Blue vulnerability, similar to how the WannaCry attack unfolded.

Talos' initial analysis pointed to the attack starting in the Ukraine, possibly from software update systems for a Ukrainian tax accounting package called MeDoc. Later, MeDoc itself confirmed those suspicions. There were other reports of this attack appearing in France, Denmark, Spain, the UK, Russia and the United States.

Again, thanks to Cisco's defense-in-depth architecture for protecting against ransomware, this attack didn't reach our customers. Cisco Network Security products (Next Generation Firewall, Next Generation Intrusion Prevention System, Meraki MX) have up-to-date rules (since the vulnerability was known in mid-April) that detect attempts to exploit MS17-010.

> “ Ransomware has been grabbing headlines and reportedly brought in more than $1 billion in 2016. Evolutions in ransomware, such as the growth of Ransomware-as-a-Service, make it easier for criminals to carry out their attacks, regardless of their skill set.

Also, the Cisco Advanced Malware Protection technology (AMP on endpoints, network, and email/web gateways) had up-to-date information on this ransomware and blocked it or prevented its execution.

From “Classic” Ransomware to “Destruction of Service”

Ransomware has been grabbing headlines and reportedly brought in more than $1 billion in 2016. Evolutions in ransomware, such as the growth of Ransomware-as-a-Service, make it easier for criminals to carry out their attacks, regardless of their skill set. Cybercrime is a big, rapidly growing business and bad actors are constantly innovating to increase their revenue. The Cisco 2017 Midyear Cybersecurity report points out several emerging ransomware tactics:

1) Adversaries are using ransomware codebases to their advantage: Malicious actors are creating malware quickly, easily, and cost-effectively by using open-source codebases, such as Hidden Tear and EDA2, which publicly release ransomware code for “educational” purposes. Adversaries tweak the code so it looks different from the original and then deploy the malware. Many of the “new” ransomware families that Cisco threat researchers have observed in recent months use open-source code from educational codebases.

2) Ransomware-as-a-service (RaaS) platforms are growing fast: RaaS platforms, such as Satan, are ideal for lazy adversaries who want to enter the ransomware market. They don't need to devote resources to developing innovative tactics. In fact, they can launch a successful campaign without having to perform any coding or programming at all. The operators of these platforms, which are growing in number, take a cut of attackers' profits. Some will even deploy the ransomware and provide additional services, such as tracking the progress of their customers' campaigns.

3) Ransomware Denial of Service (RDoS): In 2016, nearly half of all companies (49 percent) suffered at least one cyber ransom incident—either a ransomware attack (39 percent) or a ransom denial of service (RDoS) attack (17 percent). According to Radware, a gang of cybercriminals known as the Armada Collective has been responsible for most of the RDoS attacks to date. Their typical ransom demand is 10 to 200 bitcoins (one bitcoin is 3,600 USD at current rates). A short "demo" or "teaser" attack usually accompanies the ransom note. When time for payment expires, the attackers take down the target's data centres with traffic volumes typically exceeding 100 Gbps.

4) Destruction of Service (DeOS): on top of uncovering this rapid evolution of threats and increasing magnitude of attacks, the Cisco 2017 Midyear Cybersecurity Report also forecasts the rise of "destruction of service" (DeOS) attacks. These could eliminate organisations' backups and safety nets, required to restore systems and data after an attack.

IoT: Internet of Threats

On the one hand, criminals continue to increase the sophistication and intensity of attacks. On the other hand, businesses are finding it hard to keep up with even basic cybersecurity requirements. And as Information Technology (IT) and Operational Technology (OT) converge in the Internet of Things, organisations struggle to see everything in their complex infrastructures.

According to Gartner, there will be 8.4 billion connected things (devices, vehicles, buildings, sensors, you name it) in use worldwide by the end of this year, a 31 percent increase from 2016. This number will reach 20.4 billion by 2020. Also by 2020, 1 million new IoT devices will be connecting to the Internet every hour.

IoT represents a big opportunity in many areas: from industry to smart cities, from healthcare to connected homes. But as it grows, so too does the potential attack surface. Most companies don't even know which IoT devices are connected to their network. IoT devices, which include everything from cameras to thermostats to smart meters, are generally not built with security in mind. They often lag well behind desktop security capabilities and have vulnerability issues that can take months or years to resolve. In many cases, the owners of IoT devices cannot access their systems to remediate a compromise. This limitation becomes an advantage for adversaries.

This long-feared threat was brought to fruition in 2016. Hackers took control over multiple connected devices and turned them into botnets to deploy cyberattacks. A 665-Gbps attack targeted the security blogger Brian Krebs in September. Shortly thereafter, a 1-TBps attack hit the French hosting company OVH. In October 2016, DynDNS suffered an attack that caused an outage to hundreds of popular websites—the largest of the three Internet of Things (IoT) DDoS attacks.

The Mirai botnet, which was responsible for the DynDNS attack, has been infecting hundreds of thousands of IoT devices, turning them into a "zombie army" capable of launching powerful volumetric DDoS attacks. Security researchers estimate that millions of vulnerable IoT devices were actively taking part in these coordinated attacks.

IT and OT: New Allies Against Cybercrime

Security professionals in every industry are aware of the evolving sophistication of threats, and the need to stay a step ahead of adversaries. Of course, each industry faces its own unique security challenges and has different security maturity levels, but these are common concerns.

Many organisations have experienced public breaches and it is quite common for them to lose revenue, customers and business opportunities as a result. Therefore, mitigating damage and preventing similar breaches are high on the list of worries.

In many of the verticals, the need to integrate information technology (IT) and operational technology (OT) is critical – and, especially, ensuring that the integrated systems are protected. WannaCry caused shutdowns across many organisations, an example of how attacks can affect connected systems. If connectivity isn't done securely and in a coordinated fashion, then even untargeted ransomware can affect OT systems.

In the past, these technologies and their respective teams worked separately: the OT staff managed machines and plants, while IT managed enterprise business applications. Today, many OT sensors and systems are being accessed from the business side. As an example, manufacturing execution systems (MES) now seek the streams of telemetry from those sensors to better optimise and predict operations.

> “ Security professionals in every industry are aware of the evolving sophistication of threats, and the need to stay a step ahead of adversaries.

As connected systems come to the OT world, IT and OT should work together. They can benefit from sharing data for analysis to help improve safety and product quality. They can also work together to manage cybersecurity threats. To do so, they must develop their defense-in-depth capabilities, since disconnected and siloed systems won't provide a comprehensive view of IT and OT.

What Makes Cisco's Approach Unique?

The constantly changing threat landscape outlined above is not the only challenge that organisations are facing. What they are also struggling with is complexity. Large customer IT environments have security point products deployed from as many as 50 vendors, making them too difficult to manage and leaving businesses vulnerable. We call this paradox the security “effectiveness gap”.

> “ Taking a holistic approach to security helps take advantage of investments and network infrastructure already in place. It creates a force multiplier effect and reduces cost by over 30% versus a point product approach.

For each new security point product a company adds, there's only a small growth in capability but a much higher increase in complexity. Companies are deploying dozens of disparate security technologies from multiple vendors – which in turn becomes a difficult task to manage, leaving businesses at greater risk. Imagine trying to fly a plane made out of 50 different planes: that's not a solution, that's a mess.

Security teams do a noble job staying on top of dozens of consoles, thousands of uncorrelated alerts, endless logs and weeks of incident response. Yet, on average, 44 percent of security alerts go uninvestigated by security teams. This is indicative of the complexity that teams need to manage, day in and day out. Combine it with the security talent shortage and you see why this approach does not work.

Taking a holistic approach to security helps take advantage of investments and network infrastructure already in place. It creates a force multiplier effect and reduces cost by over 30% versus a point product approach. Not to mention the avoided costs of a security breach.

Cisco's strategy combines "best of breed" portfolio with an architectural approach to security, making it simple, open and automated. This means products are integrated and share context and threat information, so that if you see a threat once, you can stop it everywhere. Cisco products are also developed with the most robust trustworthy security technologies. These technologies provide enhanced security and resilience and help mitigate modern cyberattacks, counterfeit, tampering, and the unauthorized modification of hardware and software.

We understand that in order to be effective, security needs to be built into the network, and not just added on. The network is the only place that brings together all the elements for a secure digital future. Our recently announced intuitive network goes even further. It represents the culmination of Cisco's vision to create an intuitive system that anticipates actions, stops security threats in their tracks, and continues to evolve and learn. We protect customers across the extended network – including data centres, virtual environments, the cloud, mobile devices and endpoints – and throughout the entire attack continuum: before, during and after an attack:

Before (prevent): Organisations need to know what is on their network (devices, operating systems, applications and users) to be able to defend it.

During (detect): When attackers get through, organisations need to be able to detect them quickly. Once they detect an attack, they will be able to block it and defend the environment. Speed of detection is important to minimise the opportunity for damage to take place.

After (respond): Invariably, some attacks will be successful, and organizations need to be able to determine the scope of the damage, remediate, and bring operations back to normal.

The right security strategy is all about managing risk. To understand that risk, we need complete visibility of the network and what and who connects to it. This means looking at the security posture from a technology and operational perspective. It means having the right technology and processes in place to prevent, react to, and remediate threats. It also means educating employees to act in a safe manner. As such, it is important to take a holistic approach to security strategy. ■

ANALYSIS

CYBERSPACE AND INTERNATIONAL RELATIONS: DIPLOMATIC INITIATIVES TO AVOID THE RISK OF ESCALATION IN THE CYBER ARENA

LUIGI MARTINO
is the Head of the Center for Cyber Security and International Relations Studies, a specialized observatory of the CSSII, at the University of Florence. He is IP Project Manager of the joint-project OSCE-University of Florence entitled "Enhancing the Implementation of OSCE CBMs to Reduce the Risks of Conflict Stemming from the Use of ICTs". Currently, Luigi is a Ph.D. Candidate in Human Rights and Global Politics, School of Advanced Studies Sant'Anna in Pisa, with a research focus on "Improving Cybersecurity for Critical Infrastructure: The Public-Private Partnership Model Against Cyber Attacks". He is Consultant of Italian Ministry of Foreign Affairs for "cyber issues" and he is Member of the Delegation of the Italian MoFA at the G7 Ise-Shima Cyber Group.

Introduction

Subordination of war to politics has been sought since the Modern Age to put legal and military limits on violence. In this sense, international relations (the main expression of interactions between nation states) have mainly been focused on the fundamental research for international security and stability, basing the international system on shared legal and diplomatic frameworks (using a substantial body of international law and, when necessary, a pragmatic "balance of power") which have been applied, over the decades, with the ultimate aim not to eliminate war, but rather to limit and regulate the catastrophic effects of unrestricted violence[1].

However, Carl von Clausewitz described the war as a social and political activity that cannot be reduced to either art or science[2]. To paraphrase him, war has a dynamic soul that suits the times and the ways that propagate it[3]. Indeed, Clausewitz writes: "War [...] resembles a chameleon because it changes its nature in every concrete case". Indeed war – as the Prussian officer intends it – is a purely political act; it is a phenomenon intimately linked to the activity of the State, "the continuation of politics by other means"[4].

Following the Clausewitzian's approach, the rise of the cyber domain and its consequent "immersion" into international politics and the military events has also drastically changed the contemporary approach to warfare and violence. However, a proper analysis of the cyber domain reveals how the uncertainty and the intrinsic military use of civilian instruments create serious doubts over the possibility of adopting the "old rules" of legal and military limits on violence in a dimension where the concept of warfare is based on the "virtualization and anonymization" of conflicts[5]. Indeed, as Nigel Inkster has observed:

> *"The evolution of the cyber domain [...] has significantly complicated this picture, not merely in terms of how armed forces adopt and adapt to new technology, but in terms of raising questions about what constitutes military use in a domain where civilian and military users are inextricably entangled, and in which many cyber capabilities that are not obviously military in purpose can be used to generate militarily relevant effect".*

According to scholars and experts, cyberspace (after earth, sea, air and space) represents the fifth dimension

[1] | Regarding this specific point see Liang Q. and Xiangsui W., Unrestricted Warfare, PLA: Literature and Arts Publishing House, Beijing 1999.

[2] | Von Clausewitz C., On war, Princeton University Press, Princeton, N.J 1984.

[3] | Ibidem.

[4] | Ibidem.

[5] | See Williams P. and Fiddner D. (Eds.), Cyberspace: malevolent actors, criminal opportunities, and strategic competition, Strategic Studies Institute and the U.S. Army War College Press 2016.

of conflictuality[6]. Indeed, there are worrying indicators that stress the increased use of cyber tools for military purposes[7].

There is, however, a dangerous and instable situation that surrounds the cyber domain: a lack of "rules of the game". For these reasons, it is relevant to assess the international stakeholders' ability – including, in primis, the states, as well as international and non-governmental institutions (IOs and NGOs), private companies, and non-state actors – to create (or not) the "rules of the game" (i.e. the diplomatic and legal framework) in a dimension that has reached a consolidated level of militarization but, in terms of stability and security, is still comparable to an ungoverned space.

There is no doubt that cyberspace and ICT technologies have provided relevant inputs for the economic, social and individual development of contemporary societies. However, the "low" barrier of access to the development of ICTs and the complexity of the cyber environment (in particular related to anonymity), contribute to increasing sophistication of the new challenges emerging from the digital domain. More importantly, both the complexity and the current inability to attribute cyberattacks "beyond a reasonable doubt" represent the intrinsic pathologies of the cyber domain which contribute to creating a "wall" impeding dialogue, transparency, and trust between states. In addition, an increasing number of events (such as Estonia 2007, Georgia 2008, Iran 2010 and, more recently, Ukraine 2015–2017) have clearly demonstrated that it is possible to produce real effects through virtual instruments and finally, that "physical damage is already a reality"[8].

In sum, all of these events have, above all, increased policymakers' awareness of the importance to regulate the cyber domain in line with the main evidence that ungoverned cyber weapons can facilitate political and military escalation in the international arena with a pernicious effect on international peace and security[9].

UN, OSCE and G7: Diplomatic Initiatives For Stability and Cooperation in Cyberspace

To date, states have preferred to adopt the bilateral approach to govern cyber threats, considering multilateral fora as "time consuming" and "inefficient" processes. There are, however, alarming indicators showing a) how the number of cyber incidents that are threatening the security and safety of the states and citizens is dramatically increasing and b) the growing number of cases in which nation-state actors are involved in these malicious cyber events. In other words, these indicators highlight the complete failure of bilateral exercises in governing threats and challenges emerging from the cyber domain, showing how states have tried to treat the symptoms of the malady rather than its causes[10].

Noting these failures and recognizing the urgency of addressing the potential tensions arising from the ungoverned cyber domain, international actors such as the UN, the OSCE and the G7 have launched specific activities in order to enhance stability, improve cooperation, and increase trust among states in the cyber arena. These initiatives include, in general, the identification of common norms for responsible State behaviour and, in particular, measures

[6] | See Nye J., The future of power, Public Affairs, New York 2011.

[7] | According to the report 'Cyber Index', published in 2013 by the United Nations Institute for Disarmament Research (UNIDIR), around 47 UN Member States have developed ICT programs with military objectives. Some 15 of these involve offensive capabilities. See UNIDIR 'The Cyber Index International Security Trends and Realities', URL: www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf ; See moreover Meulenbelt S., The Worm as a weapon of mass destruction, "The RUSI Journal", No. 157 (2), p. 62; and Valentino- DeVries J., Thuy Vo L. and Yadron D., Cataloging the World's Cyberforces, "The Wall Street Journal" 2015, URL: http://graphics.wsj.com/world-catalogue-cyberwar-tools.

[8] | Inkster N., 2017, op. cit.

[9] | Regarding this point consider that there is in place a common file rouge which underlines the growing states' approach to address cyber attacks through an "equivalence response" that in some specific case is equivalent to a classical kinetic attack. See, for instance, the statement in the last US Department of Defense 'Cyber Strategy', published in 2015 which declares that the United States could threaten traditional kinetic attacks in response to a cyber attack, see http://archive.defense.gov/home/features/2015/0415_cyber-strategy.

[10] | See Healey J. and Maurer T., What it'll take to forge peace in cyberspace, Christian Science Monitor, March 2017.

to improve transparency in order to reduce the risks of misperception in cyberspace[11].

The first initiative was launched under the auspices of the United Nations, where in 1998, following a proposal made by the Russian Federation, the General Assembly approved Resolution no 53/70[12]. The primary objective of this resolution was to find useful mechanisms to improve international cooperation in cyberspace. Following the adoption of Resolution 53/70, the General Assembly established the Group of Government Experts (UNGGE), which is entirely focused on ICT developments in the context of global security[13]. The first UNGGE working group met in 2004, and its main objective was to study the threats and challenges to international security deriving from the malicious use of cyber tools and to propose useful actions for improving international stability and cooperation.

Published in 2010, the UNGGE report noted that "uncertainty regarding attribution and the absence of common understanding regarding acceptable state behaviour may create the risk of instability and misperception" and, in order to prevent the risk of political and military escalation, recommended "further dialogue among States to discuss norms pertaining to State use of ICTs to reduce collective risk"[14]. which would later pertain, in their 2013 report, to "rules or principles of responsible behaviour of States and confidence building measures in information space"[15].

Subsequently, in the 2013 and 2015 reports, the UNGGE highlighted, among other priorities, the need to further the analysis of the approach to making existing international law applicable to cyberspace[16]. Another key recommendation outlined in the 2015 UNGGE report was the need to provide for measures to build trust, transparency, and cooperation among States. In this regard, experts explained how:

> *Voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. They can make an important contribution to addressing the concerns of States over the use of ICTs by States and could be a significant step towards greater international security. States should consider the development of practical confidence-building measures to help increase transparency, predictability and cooperation.*

Following these initiatives promoted under the United Nations' framework, the Organization for Security and Cooperation in Europe (OSCE) launched a specific exercise to increase "confidentiality", "transparency", "trust", and "dialogue" among the 57 participating States. To this end, the OSCE, in line with the UNGGE recommendations, has started the first multilateral exercise of "cyber diplomacy" in the context of cybersecurity through specific confidence-building measures (CBMs) in order to reduce the risk of conflicts arising from the malicious use of cyber technologies[17].

This initiative started on 26 April 2012, when the OSCE created a dedicated informal working group (IWG) aimed at developing CBMs to reduce the risks of conflicts in the cyber domain[18]. The IWG's work has produced some concrete results. In 2013, all the OSCE participating States approved an initial set of 11 CBMs focused mainly on transparency measures, communication channels, and trust among States. In March 2016, they endorsed a supplementary set of CBMs[19]. The latter set focused on cooperative measures among participating States in cyberspace,

[11] | See Mayer P., Diplomatic Alternatives to Cyber-Warfare, "The RUSI Journal", No. 157 (1), p. 14; and Osula A. and Rõigas H. (Eds.), International Cyber Norms: Legal Policy and Industry Perspectives, NATO CCD COE Publications, Tallinn 2016.

[12] | See United Nations Office for Disarmament Affairs (UNODA), [online] www.un.org/disarmament/topics/informationsecurity.

[13] | See UN Report (A/65/201), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 30 July 2010, [online] http://undocs.org/A/65/201.

[14] | Ibidem.

[15] | See UN Report (A/68/98), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, [online] http://undocs.org/A/68/98.

[16] | Ibidem; moreover, see UN Report (A/70/174), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, [online] http://undocs.org/A/70/174.

[17] | See Pawlak P., Confidence-Building Measures in Cyberspace: Current Debates and Trends, Anna-Maria Osula and Henry Rõigas (Eds.), pp. 129-153, op. cit.

[18] | OSCE Permanent Council Decision no. 1039.

[19] | OSCE Permanent Council Decision no. 1106 and Permanent Council Decision no. 1202.

for instance, on mitigating cyberattacks against critical infrastructures and highlighting how such attacks could have a knock-on effect on the entire OSCE region.

The "Group of the Seven" (G7) has also moved along the path set by international initiatives to enhance diplomatic activities in cyberspace undertaken by the UN. For this purpose, the G7 leaders, during the Japanese Presidency, created the Ise-Shima Cyber Group (ISCG), a permanent working group set up by the Foreign Ministers, devoted entirely to cyber issues. The "cyber working group" met for the first time in 2017, during the G7 chaired by Italy. The Italian Presidency of the ISCG has initiated purely diplomatic initiatives in order to establish norms of responsible state behaviour in cyberspace, aligning its activities with the UNGGE recommendations. In particular, the ISCG was inspired by the 2015 UNGGE report which recommended that in order to reduce the risks and threats to international peace, security, and stability, it is vital to identify non-binding political norms of responsible State behaviour in cyberspace. In this regard, the 2015 UNGGE report states that:

> *Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.*

Under the Italian Presidency, the negotiation process started with an initial proposal based on a "code of conduct" in cyberspace, with a specific index (the so-called triage) on verification and actions to be taken in case of an attack or cyber incidents. However, the mediation between the initial proposal and the final position of the G7 members was reached in a political statement approved during the Lucca meeting of Foreign Ministers, also known as the "Lucca Declaration on Cyberspace", or "the Declaration on Responsible State Behaviour in Cyberspace", a document which was also endorsed in the Leaders' Communiqué during the Taormina meeting[21].

In essence, the "Lucca Declaration" primarily recognizes the predominant role of States in the process of building a safer and more stable cyberspace; in addition, the "Declaration" bases its legitimacy on the activities conducted by the UNGGE and the OSCE and finally recognizes the possibility of applying the existing international law to the cyber domain. However, the statement introduces the novelty that there is a political (and not merely technical) necessity to address the challenges and risks arising from the cyber arena. In other words, the work of the ISCG, conducted under the Italian Presidency, attempts put the emphasis on the need to move from a mostly technical approach (as is currently the case at the UN level where the UNGGE can only make recommendations and its ineffectiveness is evident in the lack of consensus that blocked the approval of the 2017 report) to a purely political-diplomatic process that, ultimately, leads to the approval of commonly agreed-upon voluntary "rules of conduct" (with the hope they become binding in the future) valid for the specific case of cyberspace.

Conclusions

The militarization of cyberspace, officially decreed by the NATO Summit in Warsaw in 2016[22] (but de facto sanctioned over the last decade by various military doctrines and national cyber security strategies), has removed any doubt about the intention of states to consider cyberspace

[20] | See Pawlak P., Confidence-Building Measures in Cyberspace: Current Debates and Trends, Anna-Maria Osula and Henry Rõigas (Eds.), pp. 129-153, op. cit.

[21] | See G7 Declaration on responsible states behavior in cyberspace, Lucca, 11 April 2017, [online] www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf; and Taormina Leader's Communiqué, www.g7italy.it/sites/default/files/documents/G7%20Taormina%20Leaders%27%20Communique_27052017_0.pdf.

[22] | See NATO Summit Warsaw 2016, [online] www.nato.int/cps/en/natohq/events_132023.htm; regarding the specific statement on cyberspace see CCDCOE NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, [online] https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

as a sphere of military conflicts, even if this area was originally created with purely technological features[23].

Today, it is an incontrovertible fact that the battlefield has become vitrual, just like the ability of cyber weapons to bring about real damage. The very actors in the field, even though their roles are well defined, are not the classic protagonists of international relations. The clearly defined cyber arena is encompasses with a number of stakeholders that are no longer just states, but also non-state actors, multinational companies, terrorists, individuals: all these stakeholders are confronting each other in the cyber arena without a regulatory framework. Although we are witnessing the consolidation of the (cyber) battlefield, the (cyber) weapons, and the (multi) actors, the cyber arena is chaotic and therefore dangerous due the lack of "rules of the game", an essential element for governing violence and preventing military and political escalation. The international initiatives (in progress) have paved the way for the political and diplomatic actions. Even though these are only "voluntary"initiatives, they have favoured a minimum framework for international cooperation involving top players such as China, Russia and the United States at the UN level, and Russia and the Unitied States at the OSCE level (CBMs). However, as underlined during the negotiation process of the "Lucca Declaration", states must recover their original and "genetic" prerogative also in cyberspace: the responsibility to protect themselves and their citizens, recognizing that a chaotic cyber environment can undermine international stability and national security[24].

In this sense, it can be said that the works of the last G7 meeting as well as of the UNGGE and the OSCE have facilitated the overcoming of the impasse created by the initial international debate revolving around the deceptive concept of "multistakeholderism". More importantly, these initiatives attempt to set into motion a completely different approach, with the lofty goal of initiating an appropriate political process of cyber diplomacy in order to define a clear and shared legal framework and create boundaries on what is the acceptable states' behaviour in the digital sphere.

Appendix: Diplomatic Initiatives For Stability and Cooperation in Cyberspace. ©Luigi Martino, 2017. Sources: United Nations Office for Disarmament Affairs, Organization for Security and Cooperation in Europe, G7. ■

Proposed by	Body	Document	When	Status	Commitment
UN	UN GGE	Reports on Developments in the Field of Information and Telecommunications in the Context of International Security	2010 2013 2015 2017	Approved Approved Approved Rejected	Voluntary
OSCE	IWG	Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies	2013 2016	Adopted Adopted	Voluntary
G7	Ise-Shima Cyber Group	Principles and Actions on Cyber Declaration on Responsible State Behavior in Cyberspace	2016 2017	Adopted Adopted	Voluntary

[23] See Geers K., World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, [in:] Fire-Eye Labs, 2014, [online] www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf; moreover, see Schmitt M. N. and Vihul L., Proxy wars in cyberspace: The Evolving International Law of Attribution, "Fletcher Security review" | vol I, issue II Spring 2014.

[24] See Carr M., Public-Private Partnerships in National Cyber-Security Strategies, "International Affairs" 2016, No. 92 (1), Oxford (UK), pp. 43-62.

CYBER**SEC** HUB

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum – CYBERSEC, one of the main public policy conferences on cybersecurity.

We are open to those who want to build the CYBERSEC community with us. Whether you are in academia, a CEO, an investor or the owner of a startup, you are invited to become an important part of our network. If you are interested in the project visit our website www.cybsersechub.eu or contact us at cybersechub@ik.org.pl.

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION OFFER

Subscribe now and stay up to date with the latest trends, recommendations and regulations in the area of cybersecurity. Unique European perspective, objectivity, real passion and comprehensive overview of the topic – thank to these features the European Cybersecurity Journal will provide you with an outstanding reading experience, from cover to cover.

In order to receive the ECJ, please use the online subscription form at www.cybersecforum.eu/en/subscription

NEW PRICES OF THE ECJ SUBSCRIPTION!

Annual subscription (4 issues) - electronic edition - ~~199 EUR~~ NEW PRICE €50 NEW PRICE

Annual subscription (4 issues) - hard copy - ~~199 EUR~~ NEW PRICE €149 NEW PRICE

Annual subscription (4 issues) - hard copy & electronic edition - ~~249 EUR~~ NEW PRICE €199 NEW PRICE

Follow the news @ECJournal

THE ECJ IS ADRESSED TO

- CEOs, CIOs, CSOs, CISOs, CTOs, CROs
- IT/Security Vice Presidents, Directors, Managers
- Legal Professionals
- Governance, Audit, Risk, Compliance Managers & Consultants
- Government and Regulatory Affairs Directors & Managers
- National and Local Government Officials
- Law Enforcement & Intelligence Officers
- Millitary & MoD Officials
- Internat. Organisations Reps.

FROM THE FOLLOWING SECTORS

- ICT
- Power Generation & Distribution
- Transportation
- Critical Infrastructure
- Defence & Security
- Finance & insurance
- Chemical Industries
- Mining & Petroleum
- Public Utilities
- Data Privacy
- Cybersecurity
- Manufacturing & Automotive
- Pharmaceutical

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