OAS

More rights for more people

WORKSHOP

CYBERSECURITY AND ELECTIONS:

NEW CHALLENGES AND GOOD PRACTICES FOR DEMOCRACY

April 3 and 4, 2024

In partnership with Canada

Table of Contents

WEDNESDAY

April 3, 2024

Time	Activity	Presenters
09:00 – 09:15	**Welcome**	**Welcoming remarks:** Francisco Guerrero, OAS Secretary for Strengthening Democracy (SFD). Alison August-Treppel, Executive Secretary of the Inter-American Committee against Terrorism (OAS/CICTE).
09:15 – 10:45	**Cybersecurity: global trends and challenges**	Increasingly sophisticated cyber-attacks are taking place through threats such as malware, mobile attacks, phishing, ransomware and in some cases also state-sponsored and orchestrated attacks. These have put the data and assets of government institutions and individuals at constant risk. This session will address global trends and challenges related to cybercrime, actors and motivations, as well as the impact of artificial intelligence in the field, to better understand the context in which electoral processes are currently taking place. Marnix Dekker, Head of Sector for Network and Information Systems at the European Union Agency for Cybersecurity (ENISA). Diego Subero, Cybersecurity Program Officer of OAS/CICTE. Katherina Canales Madrid, Former Director of Operations of CSIRT of the Government of Chile.
10:45 – 11:00	Break	
11:00 – 12:30	**Cybersecurity in elections: threats and impact**	Cyber-attacks can disrupt the delivery of essential services of an electoral process, undermine the integrity of elections and erode public confidence in the electoral authorities. The increasingly prominent use of technology in elections, the expansion of devices connected to the Internet on mobile platforms or applications, remote work and other social changes, increase the risks of being the target of an attack. This session will address the main threats to the critical infrastructure of an electoral process and their possible impact. Cait Conley, Senior Advisor to the Director, Cybersecurity & Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), United States Government. Tarun Chaudhary, Cybersecurity and Diplomacy Advisor, International Foundation for Electoral Systems (IFES). Kat Duffy, Senior fellow for Digital and Cyberspace policy at the Council on Foreign Relations (CFR).
12:30 – 12:40	Closing first day	

THURSDAY

April 4, 2024

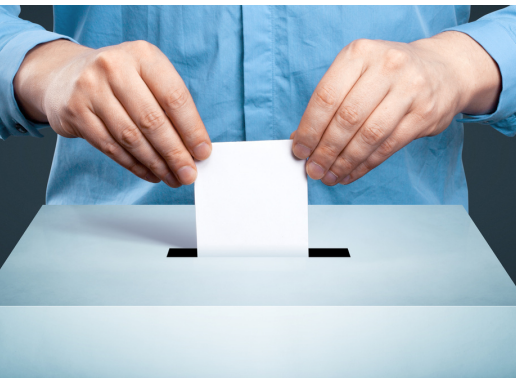
Time	Activity	Presenters
09:00 – 10:00	**Discussion Room: Cybersecurity in electoral processes**	The OAS Department of Electoral Cooperation and Observation (DECO) will give a presentation on what it has observed in terms of electoral cybersecurity policies, principles and practices in the region in recent years. Subsequently, attendees will be divided into three groups. During a 45-minute session, and with the support of facilitators and a collaborative online panel, each group will exchange views on what have been the main challenges and lessons learned in terms of cybersecurity in the electoral processes in their respective countries. Alex Bravo, Specialist of the Technical Cooperation Section, OAS/DECO.
10:00 – 10:30	**Exchange of views in the plenary session**	Workshop participants will return to the plenary to share the results of the breakout session.
10:30 – 10:45	Break	
10:45– 12:00	**Strengthening the capacities of electoral bodies to detect and effectively respond to a cyberattack: challenges, opportunities, and lessons learned**	Training of officials and voters, continuous and comprehensive risk management, inter-institutional collaboration and the exchange of experiences to improve the decision-making process are all proactive actions that can contribute to preventing or mitigating cyber-attacks. This session will address various tools or actions to strengthen the capacities of electoral bodies in this area. Peter Wolf, Principal Adviser of Elections and Digitalization at International IDEA David Yeregui Marcos del Blanco, Honorary Fellow, School of Mechanical, Aerospace and Computer Engineering, Spain Hector Hernandez, Specialists on Electoral Technology, Auditing and Cybersecurity

THURSDAY
April 4, 2024

Time	Activity	Presenters
12:00– 13:00	Case Studies: **Good practices for promoting security in cyberspace: lessons from the Americas**	Through the presentation of initiatives that have been implemented in different countries in the region, participants will deepen their knowledge on how to strengthen the capacities of electoral bodies in the face of cybersecurity threats. The experiences shared will address actions carried out at different stages of the electoral process, while focusing on different digital vulnerabilities. Afterwards, in the plenary participants will have the opportunity to present their perspectives and pose questions about the topics covered in the discussion panels. TBC Joshua Kilbert, Canadian Centre for Cyber Security
13:00 – 13:10	**Workshop Closing**	The Director of the Department of Electoral Cooperation and Observation of the OAS, Gerardo de Icaza, will deliver closing remarks to conclude this initiative. Gerardo de Icaza, Director OAS Department of Electoral Cooperation and Observation (DECO).

Concept Paper

Cybersecurity and Elections: New Challenges and Good Practices for Democracy



The Department of Electoral Cooperation and Observation (DECO) of the Organization of American States (OAS) has organized this workshop on cybersecurity in elections to promote a participatory dialogue between different actors in the region, with the aim of better understanding the trends in cybercrime at a global level, exchanging points of view regarding the impact of this matter on elections, analyzing how to counter these threats and strengthen the capacities of electoral bodies, as well as fostering strategic opportunities to promote digital integrity and security in democracy.

Through three plenary sessions of expert presentations, a discussion room among participants and a panel of case studies, attendees will be able to share knowledge and experiences, as well as generate cooperation networks for future initiatives. All workshop sessions are convened under the Chatham House Rule[1]. This workshop is made possible thanks to the generous financial support of the Government of Canada.

With the increased use of information and communication technologies, a large part of the processes associated with an election are computer-based services. The registration of voters and candidates, the tools for the control of financing, the processing and transmission of results, as well as the very mechanics of voting, are some of the examples in which technology plays or can play an essential role. However, just as information technologies can facilitate and strengthen the various stages of the electoral cycle, their scope and prevalence also increase the risks of suffering cyberattacks.

[1] This implies that participants have the right to use the information they receive, but neither the identity nor the affiliation of the speakers or participants may be revealed.

This concept paper considers some of the topics that will be addressed during the programed sessions. Its objective is not to summarize the sessions of the event, but rather to provide introductory information that could be useful for participants to reflect on prior to the workshop, as well as to prepare comments and/or questions to ask speakers or other participants.

SESSION 1 *Cybersecurity: global trends and challenges*

The current context of constant technological evolution has made cybersecurity an essential component of the digital era. The greater fluidity of information and connectivity in cyberspace has created new business opportunities and benefits for society, but it has also expanded the possibilities for crime and data manipulation, which are no longer limited to a certain geographical space or subject to a single jurisdiction. This, therefore, presents new demands for threat prevention, adoption of response strategies and promotion of trust in digital media.

Cybersecurity can be defined as "the preservation- through policy, technology, and education- of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline."[2] In addition, cybersecurity helps secure the preservation of information from its interruption, disablement, destruction, or malicious control[3].

Reports published by technology companies indicate that between 2021 and 2022 alone there was a 38% increase in cyberattacks worldwide[4], which will only increase with the continued updating and sophistication of these threats, as well as the expansion of the use of technologies such as artificial intelligence. Cybersecurity is particularly relevant for the countries of Latin America and the Caribbean, since they are a constant target of cybercriminals. The region has one of the highest growth rates in cybercrime, with some companies in the region recording up to 1,600 attacks per second.[5]

[2] Why Do We Need a New Definition for Cybersecurity? - Freedom Online Coalition

[3] Understanding Cybersecurity Throughout The Electoral Process: A Reference Document An Overview of Cyber Threats and Vulnerabilities in Elections | IFES - The International Foundation for Electoral Systems

[4] Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks

[5] NEW AQ: Hacker's Paradise: Why Latin America Is So Vulnerable (americasquarterly.org)

For these reasons, it is becoming increasingly imperative to disseminate strategies that allow continuous action to mitigate cyber risks, and to provide training to key institutions in the countries of the region to apply these strategies across all sectors of society.

The first step in preventing and combating cybersecurity threats is to know what they are and how they present themselves. Therefore, this panel aims to explore the leading trends in cybercrime and cybersecurity, in order to delve into current and future challenges. It will also be an opportunity to learn about the impact of artificial intelligence on cybersecurity.

Some of the most common risks to computer systems that will be addressed are:

- **Malware:** A program inserted into a system, usually via covert means, with the intent to compromise the confidentiality, integrity, and/ or availability of a victim's data, applications, or operating system, or to cause disruption to the victim.[6] Examples of malware are: viruses, worms, trojans, ransomware, and keyloggers.

- **Ransomware:** This is a type of malware that typically hijacks and encrypts files on a storage system, then demands a ransom, usually through cryptocurrency payments, with no guarantee that all files can be decrypted or returned in their original condition.[7]

- **Phishing:** Phishing is a cyber threat that uses social engineering techniques to trick users into revealing personally identifiable information. For example, cyber attackers send emails that result in users clicking and entering credit card data on a fake payment webpage. Phishing attacks can also result in the downloading of malicious attachments which install malware on company devices.[8]

- **DDoS:** A distributed denial of service attack (DDoS) is a coordinated effort to overwhelm a server by sending a high volume of fake requests. Such events prevent normal users from connecting or accessing the targeted server.[9] An example of this type of threat is a cyberattack targeting cloud network services that attempts to disrupt, disable, or destroy the integrity of information available on a website.

[6] Challenges and Strategies- considerations on ransomware attacks in the Americas ENG.pdf
As defined by: https://csrc.nist.gov/glossary/term/malware

[7] Challenges and Strategies- considerations on ransomware attacks in the Americas ENG.pdf

[8] What is Cyber Security? - Cyber Security Explained - AWS (amazon.com)

[9] Ibid.

SESSION 2 *Cybersecurity in elections: threats and impact*

The proliferation of IT services in the various stages of an electoral process, the expansion of devices connected to the Internet, the use of mobile platforms or applications to manage various processes and information, remote work, and other recent social changes, have increased the risks that an election could be subject to an attack. Threats to elections are not fictitious or potential but are already a reality in Latin America.[10]

Some of the ways in which cyberattacks can manifest themselves in electoral processes include:

- Theft or manipulation of information available online, including voter data.
- Attacks on the electoral body's websites, hindering public access to crucial information.
- Attacks on critical infrastructure such as power grid, telecommunications infrastructure and computer systems that may disrupt the provision of essential services.
- Intrusions in the systems of transmission, computation, tabulation, and publication of electoral results.
- DNS spoofing and poisoning, where a cybercriminal could redirect voters to a fake website that looks like the official election website, to cause voter identity theft or disruption of the voting process through flooding DNS servers with traffic.
- Conduct cyber-attacks to obtain political gain and sensitive information.
- Deficiencies with IT vulnerability management process (including zero-day vulnerabilities).
- Cybercriminals can use unsecure remote devices to gain access to the internal enterprises's network, steal information, launch an attack or disrupt the electoral process.

When cyberattacks are successful, they can undermine public confidence in the integrity of the electoral process and the electoral body. The perception that elections are not secure, or fair can significantly impact political and social stability, and undermine confidence in the democratic system.

[10] Recent examples in the region include the case of the 2018 elections in Colombia, where the Registrar's Office recorded cyberattacks days before the election (Detectan ataques cibernéticos a ente electoral de Colombia – DW – 08/03/2018); and Ecuador 2023, where the electoral authority confirmed that the telematic voting system suffered attacks from seven countries during the election day. (Voto telemático en el exterior sufrió ataques cibernéticos, confirmó la presidenta del CNE | Política | Noticias | El Universo).

DISCUSSION ROOM *Cybersecurity in electoral processes*

During this session, some of the most relevant cybersecurity vulnerabilities identified by the OAS in election matters will be addressed. These weaknesses include deficiencies in information security management; zero-day vulnerabilities; errors in configuration and programming; vulnerabilities associated with mobile devices, remote access, mobile applications (sensitive or private information); and cyberattacks directed at computer systems operating in the cloud.

After the presentation, attendees will break into three groups and for 45 minutes will exchange views on what have been the cybersecurity challenges and lessons learned in the electoral processes they have monitored in their respective countries. Please note that this discussion session is also convened under the Chatham House Rule, which implies that participants have the right to use the information they receive, but neither the identity nor the affiliation of the speakers or participants may be disclosed.

The sessions are structured around guiding questions that will stimulate the exchange of ideas. Facilitators will ask questions to the group, and participants will have a few minutes to post their comments in an easy-to-use application called padlet. This is a collaborative application in which, with just the link, participants can post in real time, ideas, comments, and even attach relevant documents, links to news or initiatives, etc. Likewise, participants will be able to make verbal interventions to share experiences from their own realities.

Some of the questions that will guide the discussion in this session, are:

- How has the institution to which you belong worked on cybersecurity issues? Is there any specific care aimed at election periods?
- Have you observed in your country any recent cyber threats that have impacted government services? If so, have any of them been targeted at the electoral body?
- What do you consider the biggest challenges facing elections in cybersecurity issues?

SESSION 3

Strengthening the capacities of electoral bodies to detect and effectively respond to a cyberattack: challenges, opportunities, and lessons learned

Strengthening cybersecurity in elections requires a proactive stance that permits mitigation of the effects of cyber threats, adopts robust measures for their prevention, and prepares for contingency and strategic incident responses. While technological complexity and rapidly evolving threats are ongoing challenges, there are opportunities for improvement and good practices that can be adopted to address these challenges.

One of the difficulties faced by many electoral bodies is the lack of capacity or resources, both financial and of personnel, to enable or maintain cybersecurity programs. Strategic partnerships with other governmental institutions, civil society organizations or technical cooperation with international organizations, are presented as an alternative to ensure the implementation of digital security measures. Shared responsibility can even be promoted by policy makers when it does not exist spontaneously.[11]

The adoption of secure technologies, as well as reviewing and updating them in the face of possible vulnerabilities, is an important step towards the protection of electoral processes. However, this step must also be accompanied by the training of electoral officials so that they are aware of existing threats and ways to prevent them. Digital education contributes to the prevention of human errors that may include: the design, configuration and programming of systems; poor testing and quality control; mismanagement of users and systems, misuse and exposure of systems to malware.

In fact, training and dissemination of information through workshops and public awareness campaigns are also essential for citizens, journalists, candidates, and other political actors, as a way to promote cyber hygiene and strengthen security throughout the electoral process.

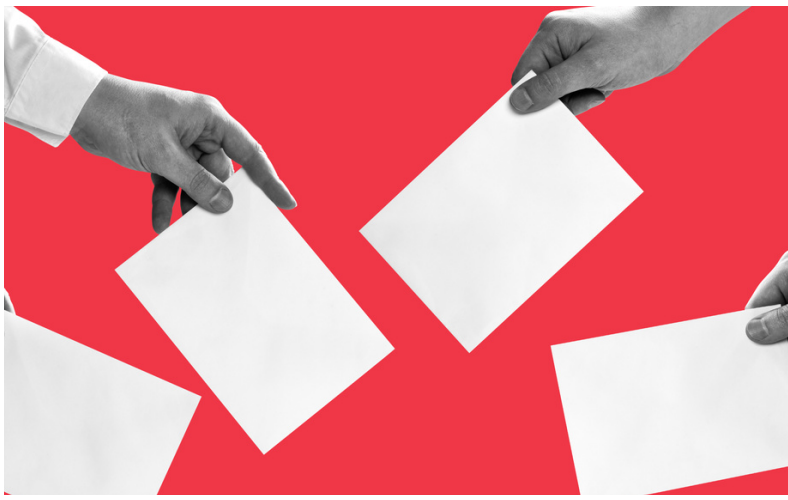
Cybersecurity management must be continuous, and not just during elections, seeking constant evaluation and feedback about how to improve and consolidate any measures adopted. In the same way, adopting a transparent posture and managing public perceptions about cyber threats to an electoral process play a fundamental role for instilling confidence in the process, and are almost as important as defending against the threats themselves[12].

[11] Cybersecurity in Elections (idea.int)

[12] Ibid.

In summary, electoral cybersecurity is essential to preserving the integrity and stability of democratic processes in an increasingly digital environment. Strengthening the capacities of electoral bodies in cybersecurity involves a combination of awareness, collaboration, and the adoption of good practices and continuous learning.

This panel aims to address the main concepts, decisions, and tools that an electoral body needs to adopt for an effective cybersecurity strategy, taking into account the limitations, opportunities and experiences in the field.



CASE STUDIES

Good practices for promoting security in cyberspace: lessons from the Americas

In this session, participants will be able to deepen their knowledge about strengthening the capacities of electoral bodies against cybersecurity threats by discussing past and current initiatives that have been implemented in different countries of the region. The experiences shared will address actions carried out at different stages of the electoral process, focusing on different digital vulnerabilities. Immediately after this session, participants will have the opportunity in the plenary to present their views and questions regarding the day's panel discussions. The case studies to be considered are:

- **Canadian Centre for Cyber Security**
- **TBC**

Panelists

FRANCISCO GUERRERO

Secretary for Strengthening Democracy of the OAS

Holds a Ph.D. in International Relations and M.A. in International Conflict Analysis, both from the University of Kent in Canterbury, England. He holds a law degree with honors from the National Autonomous University of Mexico (UNAM). He is an expert in electoral affairs, public policy, international affairs, democracy and political transition, government, and transparency. He served as Electoral Advisor of the Electoral Federal Institute of Mexico from 2008 to 2013.

In the academic field, he was founder and coordinator of the Doctoral Program in Strategic Management and Development Policy and the Master's in Economics and Government, as well as holder of the Chair of Structural Reforms of the School of Economics and Business of the University Anáhuac México Norte. He has been academic coordinator of several courses, seminars, and diploma programs; visiting researcher in several countries; and has taught classes at the doctoral, master, and undergraduate levels. In January 2008, he was selected as one of the five Mexican recipients of the prestigious Eisenhower Fellowship. He has written articles for several national newspapers in Mexico, magazines, and specialized publications. He is a weekly contributor to the newspaper Excelsior with the column Punto de equilibrio.

ALISON AUGUST TREPPEL

Executive Secretary of the Inter-American Committee against Terrorism of the OAS

Alison August Treppel has served as the Executive Secretary of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States since August 2016, where she is responsible for promoting the OAS's counter-terrorism agenda throughout Latin America and the Caribbean, and for leading OAS technical assistance efforts in such areas as cybersecurity, border management, the prevention of terrorism finance and the proliferation of weapons of mass destruction, among others.

A native of the United States, Mrs. Treppel has nearly 30 years of experience working within the inter-American system, the last 15 of which have been dedicated to multidimensional security. As Section Chief and later Deputy Director of the OAS Department of Public Security from 2006 to 2016, she supported efforts to prevent and counter threats to citizen security, including firearms trafficking, human trafficking and other manifestations of transnational organized crime. She has also served as political liaison to numerous OAS security-related bodies, including the Committee on Hemispheric Security.

Mrs. Treppel holds a B.A degree in International Relations and Spanish from Dickinson College and completed an executive education program in international and national security from Harvard University's Kennedy School of Government.

Panelists

KATHERINA CANALES MADRID

Former Director of Operations of CSIRT of the government of Chile

Katherina is a specialist in cybersecurity and has vast experience in the creation, linkage, and implementation of cybersecurity public policies. Recognized as an outstanding woman in cybersecurity in Chile, and Top Women in Cybersecurity in Latin America. She was operational director of the CSIRT of the Government of Chile, leader in the implementation of cybersecurity awareness programs, expert in cybersecurity strategies, with special emphasis on the creation, implementation, and maturation of cybersecurity incident response teams. Among her professional achievements are: the creation and legitimization of the CSIRT of the Government of Chile, co-authorship of the cybercrime law, the draft cybersecurity framework law and related sectorial regulation. She is a recognized national and international columnist and rapporteur specialized in cybersecurity.

MARNIX DEKKER

Head of Sector for Network and Information Systems at the European Union Agency for Cybersecurity (ENISA)

Marnix works at ENISA, the European Union Agency for Cybersecurity, where he is the Head of Sector for Network and Information Systems, leading a team of experts supporting the national cybersecurity authorities with implementing the NIS Directive. Their focus is on raising cybersecurity and resilience in the EU's critical sectors, covering telecommunications, internet infrastructures, trust, energy, health, transport, etc. Together with the national authorities, they work on technical issues (e.g., the EU's 5G toolbox, supply chain security), and also policy implementation (e.g. the NIS2, the EU wallet toolbox). Marnix has a Ph.D. in Computer Security and a Master degree in Theoretical physics (Quantum Physics). He left ENISA for a few years to work at the European Commission's CISO office, where he helped build up the corporate IT security function, developed the corporate IT security strategy, and acted as the link between the operational security teams and the Commission's senior management. Before joining ENISA he worked as an IT auditor at KPMG in The Hague, as an architect and protocol designer for the Dutch government's e-ID systems, and as a software developer in Italy.

DIEGO SUBERO

OAS/CICTE Cybersecurity Program Officer

Systems engineer who for more than 16 years has worked in the area of information security, especially in the field of cyber incident management in the region. For the last 10 years he has been the Cybersecurity Program Officer at the Inter-American Committee against Terrorism (CICTE) of the OAS.

His main objective is to lead projects aimed at developing technical capabilities in computer security incident response teams (CSIRTs) in Latin America and the Caribbean. He also promoted the creation of the CSIRTAmericas Network to foster regional cooperation and facilitate operational channels for the exchange of cyber threats and incidents among OAS Member States.

Panelists

CAIT CONLEY

Senior Advisor to the Director, Cybersecurity & Infrastructure Security Agency (CISA) of the United States

Cait Conley is the Senior Advisor to the Director, a role that includes responsibilities supporting CISA's election security efforts. Conley leads CISA's work in partnering with state and local election officials to manage and reduce risk to the Nation's election infrastructure.

Conley brings a wealth of election security experience and knowledge to this role having previously served as the Executive Director of the bipartisan Defending Digital Democracy Project, based out of Harvard University's Belfer Center. As Executive Director, she led the development and implementation of strategies, tools and recommendations for election administrators, election infrastructure providers, campaign organizations and leaders involved in democratic processes to better defend against cybersecurity threats. Conley is an experienced combat veteran with demonstrated leadership in global special operations, cyber operations, and counterterrorism. Most recently, Conley served as the Director for Counterterrorism for the National Security Council prior to joining CISA as a Senior Advisor to the CISA Director.

Conley is a graduate of the United States Military Academy at West Point and holds a Master's degree in Business Administration from the Massachusetts Institute of Technology and a Master of Public Policy Degree from Harvard University's Kennedy School of Government.

TARUN CHAUDHARY

Cybersecurity and Diplomacy Advisor to the International Foundation for Electoral Systems (IFES)

In his role, Dr. Chaudhary provides expert cybersecurity technical and programmatic advice across IFES' portfolio of activities and to their global constituency of partners. Dr. Chaudhary also concentrates on growing and maturing IFES' thought leadership and research within the space of electoral cybersecurity as part of IFES' Center of Cyber and Information Integrity.

Before arriving at IFES, Dr. Chaudhary worked at the US Department of Energy. He also has 15 years of broad defense industry consulting experience having provided expert consulting services to a wide variety of clients including the Office of Net Assessment within the Pentagon, large defense prime contractors and many other foreign and domestic clients.

Dr. Chaudhary has a Ph.D. in International Affairs, Science and Technology from the Georgia Institute of Technology in Atlanta, where he also received a MS and a BS. His research focuses on how cybersecurity professionals organize and collaborate to recognize and remediate large-scale problems central to the Internet's continued function. Dr. Chaudhary has been the recipient of a number of scholarships, fellowships and awards including the National Science Foundation Cyber Corps Scholarship for Service, the NNSA Graduate Fellowship and others. He has published work in the Oxford Journal of Cyber Security and co-authored numerous reports for the U.S. Department of Defense. He also maintains a Global Information Assurance Certification (GIAC) as a Global Information Security Professional (GISP).

Panelists

KAT DUFFY

senior fellow for digital and cyberspace policy at the Council on Foreign Relations (CFR)

Kat Duffy has more than two decades of experience operating at the nexus of emerging technology, democratic principles, corporate responsibility, and human rights. In 2023, she directed the Task Force for a Trustworthy Future Web at the Atlantic Council's Digital Forensic Research Lab, where she served as a resident senior fellow and published the Task Force's comprehensive report, Scaling Trust on the Web. Through previous work at the U.S. Department of State and in the nonprofit sector, Duffy has overseen the implementation of more than $100 million in foreign assistance and philanthropic funding across more than 60 countries, with a particular focus on supporting human rights defenders and journalists and civil society initiatives to improve digital security, circumvention technology, digital rights, and platform governance. Her work included some of the first public-private partnerships between high-risk civil society actors in emerging markets and private cybersecurity firms.

Duffy began her international career in Colombia, where she served as a junior professional officer with the UN High Commissioner for Refugees. She served for five years on the board of the Global Network Initiative, a platform that helps technology companies respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications. She has also served as an expert advisor for the World Economic Forum's Partnering with Civil Society in the Fourth Industrial Revolution Initiative, and has lectured at Yale, Stanford, and Georgetown Universities on technology policy and innovation.

Duffy received her BA from Yale University and her JD from the University of Michigan. In addition to the U.S., she has lived and worked in Colombia, Cuba, South Africa, and Tunisia, and is a proud "trailing spouse" within the U.S. foreign service.

ALEX BRAVO

Specialist of the Department of Electoral Cooperation and Observation of the OAS

A specialist in DECO since August 2009. He is responsible for managing projects in the areas of technical cooperation, electoral technology observation, comprehensive audits of electoral registries and software generation for the management of electoral technical cooperation. Alex is a computer science engineer; he did his undergraduate studies at the University of Maryland and holds a Master of Science in Computer Security from George Washington University.

Panelists

PETER WOLF

Principal Adviser, Elections and Digitalization at International IDEA

Peter Wolf is the Principal Adviser on Elections and Digitalization and works in the global Electoral Processes Programme at the International IDEA headquarters in Stockholm, Sweden. His work focuses on the application and impact of digital technologies in elections, emerging challenges and the trusted implementation of ICTs in electoral processes. He is the author of numerous publications, including on biometrics, cybersecurity, certification, electronic voting, open data, open source technology, special voting arrangements and electoral management.

Wolf's previous experience includes his tenure with the Elections Department of the OSCE Mission to Bosnia and Herzegovina. He has served in international election observation missions on all continents as voter registration and electronic voting expert and worked as a consultant and technology expert in election assistance projects since the late 1990s.

DAVID YEREGUI MARCOS

Honorary Fellow, School of Mechanical, Aerospace and Computer Engineering, Spain

Dr. David Yeregui Marcos del Blanco is a Process and Robotics Engineer and PhD in Production and Computing Engineering with honors. He also holds an M.Sc. Degree in International Business Management from the ICEX (Ministry of Industry, Tourism and Commerce of Spain). David has co-authored over 20 research articles in high-impact journals in the Cybersecurity, Machine Learning and Biotech fields. David has been a resident in Japan since 2006, having worked as a Trading Officer for Industry and Investment at the Economic and Commercial Office of the Embassy of Spain in Japan in 2006-2008. Subsequently, he established the Science and Technology Department of the Instituto Cervantes in Tokyo, being its first director. In 2008, he co-founded the biotech group Genhelix, devoted to the development and manufacturing of Monoclonal Antibodies and other biological therapies against cancer and auto-immune diseases. Genhelix is currently part of Fresenius Kabi and valued at over 1Billion. USD.

Currently, he is Executive Committee Member, Entrepreneur in Residence and Professor at IE University, Honorary Fellow at Universidad de León in Spain and has been Consultant for the Organization of American States (OAS) for the project "Cybersecurity applied to Electoral Processes in Latin American and the Caribbean Region". Additionally, David is Senior Advisor

Panelists

HÉCTOR TEODORO HERNÁNDEZ

Specialist on Electoral Technology, Auditing and Cybersecurity of the OAS

He is a computer expert and auditor, specialist in electronic voting and electoral technology. He is a university expert in ethical hacking, information security and security of mobile devices, and a master in professional testing. He holds a university diploma in Implementation and Auditing of Information Security Management Systems under ISO/IEC 27001 from the National Technological University in Argentina, a diploma in Enterprise Resource Planning from the National University of Cordoba and a diploma in Computer Forensics. He has national degree in Computer Systems Analyst Programmer and a Master's degree in Security, Auditing and Computer Expertise ESAPI.

He also holds international certifications in security and good IT practices such as: Lead Auditor ISO 27001, PCI DSS Implanter certificate and ITIL Best Practices certificate EXIN Holland. He also has the official certifications in cybersecurity: Certified cyber security management professional, certified information security management professional, blockchain professional certified.

Panelists

GERARDO DE ICAZA

Director of the Department of Electoral Cooperation and Observation of the OAS

Gerardo de Icaza has been Director of the Department of Electoral Cooperation and Observation since March 1, 2014. In his position as Director, he has led more than 100 Electoral Observation Missions in 27 countries. Between February and July 2018, he served as Acting Secretary for Strengthening Democracy. Previously, at the National Electoral Institute (INE) of Mexico, he served as Deputy Director of Regulations in the Coordination of the Vote of Mexican Residents Abroad and as Coordinator of the Technical Committee of Specialists for the Vote of Mexican Residents Abroad. He was also Secretary of Study and Account, and Head of the International Affairs Unit in the Electoral Tribunal of Mexico. He holds a Bachelor's Degree in Law and a Master's Degree in International Relations and Communication. He has been a university professor and is a renowned international lecturer. His most recent publication "International Law of Democracy" coordinated with Luis Almagro, is one of his numerous academic publications on democracy and electoral systems.

CRISTÓBAL FERNÁNDEZ

Jefe de la Sección de Cooperación Técnica, DECO/OEA

A lawyer by profession, he completed his higher education at the Faculty of Law of the University of Chile and has an LL.M. in International Law from American University. He has participated in more than 25 Electoral Observation Missions, being Deputy Chief of Mission in several EOMs in Colombia, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic. As Head of the Technical Cooperation Section of the Department for Electoral Cooperation and Observation (DECO) of the Organization of American States, he coordinates the electoral cooperation projects that the OAS implements in its Member States. He has led projects, provided technical support and participated in cooperation activities in various countries in Latin America and the Caribbean, on topics such as electoral registration, electoral organization, electoral justice, electoral technology, women's political participation, combating disinformation and electoral reforms. He is co-author of the methodology to observe the electoral participation of Indigenous and Afro-descendant Peoples, as well as the "Guide for organizing elections during a pandemic."

WORKSHOP

CYBERSECURITY AND ELECTIONS:

NEW CHALLENGES AND GOOD PRACTICES FOR DEMOCRACY

OAS More rights for more people

In partnership with Canada